TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Johan Skytte poliitikauuringute instituut

Peeter Leets

INDIVIDUAALSE HÄÄLE VERIFITSEERIMISE VÕIMALUSE MÕJU USALDUSELE E-VALIMISTE VASTU

Bakalaureusetöö

Juhendaja: Mihkel Solvak, PhD

Tartu 2020

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite seisukohad, ning kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

Peeter Leets, 15.05.2020

/*töö autori allkiri*/

Kaitsmine toimub ...../*kuupäev*/ kell ...../*kellaaeg*/
...../*aadress*/ auditooriumis ...../*number*/.

Retsensent: ..... /*nimi*/ (...../*teaduskraad*/),
..... /*amet*/

Lühikokkuvõte

Individuaalse hääle verifitseerimine on komponent turvalisest e-valimissüsteemist, millel on kaks põhilist ülesannet: süsteemivastaste rünnete tuvastamine ning e-hääletaja usalduse tõstmine e-valimiste vastu. Käesolev uurimus keskendub viimasele ning püüab empiirilistele andmetele tuginedes seletada, kas ja mil määral on Eestis 2013. aastal kasutusele võetud verifitseerimine valija usaldustaset mõjutanud. Usalduse ja verifitseerimise vahelist seost uurisid 2016. aastal põgusalt Mihkel Solvak ja Kristjan Vassil. Toona kolme üleriigilise valimise põhjal tehtud uuring näitas, et verifitseerimise kasutamine usaldusele olulist mõju ei avaldanud, sest rakendust kasutas väga väike ja unikaalne grupp e-hääletajaid, keda iseloomustas muuhulgas kõrge arvutikasutusoskus ning kalduvus e-valimisi juba eos usaldada.

Kuna tehnoloogia areneb tänapäeval kiiresti, oli paslik nüüd, neli aastat hiljem, verifitseerimise ja valija usalduse vaheline seos taas luubi alla võtta. Käesolevas töös analüüsiti valimisjärgseid läbilõikeküsitlusi ja tõlgendati tulemusi tehnoloogia usaldust ja difusiooni seletavate teooriatega. Selgus, et verifitseerimine on varajases innovatsioonijärgus ning seda kasutab endiselt väga spetsiifiliste tunnuste ja kõrge usaldustasemega e-valijate grupp, mistõttu efekt valija usaldustasemele tegelikkuses praktiliselt puudub. Asjaolu, et verifitseerimine ei ole kuute valimiste jooksul laiema kasutajaskonna seas levima hakanud, võib tähendada seda, et rakendus ei pruugi sellisel kujul ka tulevikus valija usaldustaset mõjutama hakata.

Sisukord

Sissejuhatus

2005. aastal sai Eestist esimene riik maailmas, kus rahvas sai üleriigilistel valimistel legaalselt siduvalt hääletada interneti teel (Solvak & Vassil 2016: 2). Peale edukat debüüti on elektroonilise hääletamise tehnoloogia kasutusel olnud kõigil, kokku üheteistkümnetel üleriigilistel valimistel. E-hääletanute osakaal on olnud stabiilselt tõusvas trendis ning 2019. aasta europarlamendi valimistel hääletas elektrooniliselt juba pea 50% valimistel osalenud hääletajatest (Elektroonilise hääletamise statistika).

E-valimiste edulugu ja valimistulemuste üha suurem sõltuvus elektroonilisest valimissüsteemist on koondanud avalikkuse tähelepanu süsteemi läbipaistvusele ja terviklikkusele. Lisaks keerulisematele, andmeturbe valdkonda kuuluvatele põhjustele, ajendas pidev privaatsuse ja turvalisuse teemaline arutelu administraatoreid välja töötama universaalse kontrollimismehhanismi, mille abil saaks nii valimiste organisaator kui ka valija veenduda süsteemi terviklikkuses ning selles, et süsteem representeerib laitmatu korrektsusega valijaskonna tegelikku valikut. Selline mehhanism, tuntud kui otsast-otsani verifitseerimine, lubab valimiste korraldajal efektiivselt tuvastada süsteemiründe id ning e-hääletajal veenduda selles, et tema hääl jõuab korrektsel kujul süsteemi andmebaasi (Vabariigi Valimiskomisjon 2013: 17-18). E-hääletajale suunatud funktsionaalsus peaks teoreetiliselt valija usaldust kogu süsteemi suhtes tõstma, sest valijale kinnitatakse, et hääletamise protsess toimus oodatult (Solvak & Vassil 2016: 128).

Verifitseerimise mõju Eesti e-hääletaja usaldusele on varasemalt uurinud Mihkel Solvak ja Kristjan Vassil (2016: 132-141), kelle tulemused ja järeldused on käesoleva töö peamiseks teoreetiliseks lähtekohaks. Toona viitas analüüs sellele, et verifitseerimist kasutab mõneti paradoksaalselt vaid kitsas grupp e-valijaid, kelle usaldus e-valimiste vastu on niigi kõrge, mistõttu ei avalda verifitseerimine kogu e-valijaskonna usaldustasemele olulist mõju (Solvak & Vassil 2016: 140). Nagu kipub olema kõigega, võtab ühiskonnas uue tehnoloogia omaks võtmine aega, ning toona oli veel lahtine, kas verifitseerimine suudab üldse kunagi valija usaldustaset arvestataval määral mõjutada (Solvak & Vassil 2016: 141). Uuringud on näidanud, et elektroonilise valimise tehnoloogia hakkab laiema valijaskonna seas kanda kinnitama vähemalt kolme valimise

möödudes (Solvak & Vassil 2016: 4). Tänaseks on verifitseerimist kasutatud kokku kuutel üleriigilistel valimistel, mistõttu on põhjust verifitseerimine uuesti luubi alla võtta ning uurida, kas ja mil määral on rakendus tänaseks oma sekundaarset eesmärki, e-valija usalduse tõstmist, täitma hakanud.

Käesoleva uurimistöö eesmärk on küsitlusandmete kvantitatiivsele analüüsile toetudes välja selgitada, kas ja kuidas mõjutab verifitseerimise võimalus e-hääletaja usaldust e-valimissüsteemi vastu. Uuritakse, milline inimtüüp on altim verifitseerimist proovima ning kuidas erineb verifitseerimisest mitteteadlike e-hääletajate usaldus nende e-hääletajate usaldusest, kes a) teavad verifitseerimisest b) kasutavad verifitseerimist.

Töö analüüsiosa baseerub läbilõikelise valimisjärgse küsitlusuuringu tulemustel (2005-2019), kust enamasti kasutati verifitseerimisjärgsest perioodist (2013-2019) pärinevaid andmeid. Andmeanalüüsiks kasutati statistilise andmetöötluse paketti RStudio. Kuna küsitlusandmeid koguti ainult peale igat valimist, ei olnud paraku võimalik võrrelda kas valija usaldustase on vahetult enne ja pärast e-hääletamist ja verifitseerimist muutunud. Sellegipoolest oli võimalik varasema uuringu tulemusi käesoleva töö omadega kõrvutades ja tehnoloogilist difusiooni käsitleva teooria abil verifitseerimise ja usalduse vahelist interaktsiooni seletades piisavalt ammendavaid järeldusi teha.

Töö on struktureeritud viieks osaks. Esimeses peatükis selgitatakse teooriale tuginedes, millest sõltub valija usaldus verifitseerimise ja e-valimissüsteemi vastu üldiselt ning kuidas peaks verifitseerimise kui tehnoloogilise innovatsiooni levik ajas kulgema. Teises peatükis püstitatakse konkreetsed uurimisküsimused ja teooriast lähtuvad hüpoteesid. Kolmandas peatükis tutvustatakse töö metoodikat, kvantitatiivseks andmeanalüüsiks kasutatud vahendeid ning valimit. Neljandas peatükis visualiseeritakse ja kirjeldatakse andmeanalüüsi tulemusi. Viiendas peatükis formuleeritakse analüüsi tulemustest järeldused, kõrvutatakse neid teooriaga ning vastatakse uurimisküsimustele.

1 Teoreetiline osa

1.1 Individuaalse hääle verifitseerimise olemus ja definitsioon

Elektrooniline hääletamine on oma olemuselt ohtlikum ja haavatavam süsteem kui paberhääletamine, sest käega katsutava tõendusmaterjali puudumine tekitab vajaduse usaldada tehnoloogilist süsteemi (Heiberg & Willemson 2014: 1). Vigane või pahavaraga nakkunud hääletusseade võib hääletussedelit ilma jälgi jätmata mõjutada (*Ibid.*). E-hääletamise puhul varitsevad häält tema teekonna jooksul erinevad ohud, mis võivad hääletustulemust ja kogu süsteemi terviklikkust kahjustada (Al-Shammari et al. 2012: 437):

1. Tehnilised süsteemivead – tarkvaralised vead, füüsilise masina vead, pahavarad hääletamiseks kasutatavas masinas või valimissüsteemi serveris, süsteemi rünnakud (*Ibid.*).
2. Protseduurilised vead – võimalus, et üks või teine osapool on hääletamisprotsessis korruptiivne või ebaaus (*Ibid.*).

Kogu süsteemi terviklikkus ei saa baseeruda pelgalt rahva heal usul, et kõik töötab, nagu peab. (Solvak & Vassil 2016: 55). 2011. aasta Riigikogu valimised sattusid hääli manipuleeriva pahavara ohvriks, mis lõppes poliitiliselt motiveeritud püüdlustega tühistada kogu e-hääletuse tulemused (Heiberg & Willemson 2014: 1). Kuigi hääletustulemuste kompromiteerituseks piisab vaid teoreetilisest võimalusest, et süsteemis on nõrk koht, viitasid konkreetsed juhtumid sellele, et e-valimissüsteem vajab mehhanismi, millega saaks süsteemi töö korrektsust efektiivselt kontrollida.

Taolise kontrolli rakendamiseks peab e-valimissüsteem olema otsast-otsani[1] (edaspidi E2E) verifitseeritav (Rura et al. 2011: 125). E2E verifitseerimisel on kaks keskset ideed – universaalne verifitseeritavus, ehk igaüks saab veenduda, et valimistulemuste arvutamisel arvestati korrektselt kõiki kehtivaid hääli; individuaalse hääle verifitseeritavus, ehk üksikhääletaja saab veenduda, et valimissüsteem luges ja talletas

[1] Ing k. *end-to-end*

korrektselt tema enda hääle (Gibson et al. 2016: 281). Parasjagu kasutatav verifitseerimissüsteem lähtub konkreetse valimissüsteemi vajadusest ja võimalustest, mistõttu ei ole verifitseerimise definitsioon alati ühene (Heiberg & Willemson 2014: 2). Sven Heiberg ja Jan Willemson (*Ibid.*) toetuvad Eesti verifitseerimissüsteemi määratlemisel Popoveniuc et al. (2010) E2E verifitseerimise mittefunktsionaalseid nõudeid[2] kirjeldavale definitsioonile, mille järgi loetakse individuaalse hääle verifitseerimise võimalus valimistel täielikult kättesaadavaks siis, kui on võimalik kontrollida, et:

1. **Esitatud hääletussedelid on korrektselt sõnastatud** – mõlemad osapooled, nii hääletaja kui ka lugemissüsteem, loevad ja mõistavad selle sisu üheselt. (Popoveniuc et al. 2010: 4).
2. **Süsteemile edastatud hääletussedelid on samuti korrektsed** – edastatud häälte hulgas ei tohi olla kattuvaid või negatiivseid hääli (*Ibid.*) Lugemissüsteemis peab eksisteerima kontroll, mis tagab, et krüpteeritud hääle väärtus ei representeeri süsteemi jaoks võimalust, kus hääletaja saab valitud kandidaadi poolt hääletada rohkem, kui lubatud, või hääletada sootuks kandidaadi vastu (Popoveniuc et al. 2010: 7).
3. **Hääl loetakse korrektselt ära** – hääletussüsteem loeb ja jätab meelde täpselt selle väärtuse, mis süsteemile edastati (Popoveniuc et al. 2010: 4).
4. **Koondtulemus arvutatakse korrektselt**, ehk hääletuse tulemus reflekteerib süsteemile edastatud hääletussedelite koguarvu (*Ibid.*). See on universaalselt verifitseeritavas hääletussüsteemis kontrollitav ka nende poolt, kes ei hääletanud, sest hääletustulemused on avalikud (*Ibid.*).
5. **Eksisteerib süsteemne järjepidevus** – koondtulemuse arvutamise kontrolli suunatud hääletussedelite hulk peab ühtima algselt süsteemile edastatud hääletussedelite hulgaga ja vastupidi (Popoveniuc et al. 2010: 5).
6. **Kontrollitakse eranditult iga hääletussedeli korrektsust** – mitte ühtegi hääletussedelit, mida ei saa verifitseerida, ei kaasata koondtulemuse arvutamise protsessi (*Ibid.*).

[2] Ing k. *performance requirements*

Verifitseerimise olulisim efekt on hääletatamiseks kasutatavatele füüsilistele masinatele suunatud ulatuslike ja valimistulemusi potentsiaalselt mõjutavate rünnakute tuvastamine (Vabariigi Valimiskomisjon 2013: 18). „Kui kasvõi 5% e-hääletajatest oma häält kontrollib, muutub ulatuslike rünnete märkamatu teostamine võimatuks“ (*Ibid.*). Vigade ja rünnete tuvastamise efekt tekitatakse seega rakenduse kasutajate kaudu – kui kasvõi ühe e-hääletaja verifitseerimise tulemus on oodatust erinev, on see indikaatoriks, et midagi võib olla valesti. Samuti võimaldab E2E verifitseeritav valimissüsteem korduvat hääletamist, mis leevendab teatud määral e-valimiste puhul aktuaalseid sunniviisilise hääletamise ja häälte ostmise probleeme (Joaquim et al. 2013: 170). Teisisõnu, kui valija tunneb, et tema otsust mõjutati, saab ta hiljem uuesti hääletada ja arvesse võetakse viimasena antud hääl (Heiberg & Willemson 2014: 1). Verifitseerimine aitab seeläbi säilitada valimistulemuste terviklikkust, mis peaks tõstma e-hääletaja usaldust süsteemi vastu (Rura et al. 2011: 125).

1.2 Verifitseerimine Eestis

Individuaalse hääle verifitseerimise võimalus võeti Eestis esimest korda kasutusele 2013. aasta kohalike omavalitsuste valimistel (Solvak & Vassil 2016: 127). Eesti e-valimiste verifitseerimissüsteem ei täitnud esialgu kõiki eelnevas peatükis kirjeldatud nõudeid, kuid kaks põhilist elementi olid olemas - võimalus kontrollida, kas hääletaja valik 1) edastati süsteemile korrektsel kujul 2) talletati vastaval kujul süsteemi serveris (*Ibid.*) (definitsioonis punktid 1 ja 3). Eestis on täpne hääle verifitseerimise protseduur kasutaja tasemel järgnev (Heiberg & Willemson 2014: 3):

1. Valija tuvastab keskserverile oma isiku;
2. Valijale edastatakse nimekiri L kandidaatidest;
3. Valija teeb oma valiku c_v ja saadab allkirjastatud hääle b_{anon} serverisse, krüpteerituna juhuslikult genereeritud arvujada r kaudu;
4. Server tagastab valijale unikaalse juhuslikult genereeritud viite häälele vr, viide ja arvujada kuvatakse kasutajale QR-koodina;
5. Valija viib viite vr ja arvujada r üle nutiseadmesse (skänneerib QR-koodi);
6. Valija nutiseade saadab keskserverile viite vr;

7. Valija nutiseade saab vastu hääle b_{anon}, mis vastab keskserveris viitele *vr*, koos kandidaatide nimekirjaga *L;*
8. Nutiseade arvutab iga kandidaadi $c \in L$ kohta krüpteeritud väärtuse, kasutades krüptovõtmena arvujada *r* – kui ühe kandidaadi c' kohta arvutatud krüpteeritud väärtus kattub häälega b_{anon}, siis kandidaat c' kuvatakse kasutajale ning kui $c_v = c'$, siis ühtib edastatud hääl hääletaja algse valikuga.

Avalik elektroonilise hääletamise statistika viitab sellele, et verifitseerimine on Eestis alles nišistaatuses. Kasutajate hulk on tänaseni jäänud pigem tagasihoidlikuks ning verifitseerimine ei ole osutunud kaugeltki sama populaarseks innovatsiooniks kui e-hääletamine ise. 2013. aasta kohalike omavalitsuste valimistel (KOV), kus elektrooniliselt hääletas 21,2% valijatest, kasutas verifitseerimist 3,4% kõigist e-hääletanutest (Tabel 1.1). Kui e-hääletajate osakaal kõigist osalenud hääletajatest on e-valimissüsteemi rakendamisest alates stabiilselt tõusnud (keskmiselt 6,3% võrra iga valimisega), siis verifitseerijate osakaal kõigist e-hääletanutest ei ole kuue vaatlusaluse juhtumi põhjal oluliselt muutunud, tõustes iga valimisega keskmiselt vaid 0,5% võrra.

Tabel 1.1: E-hääletajate ja verifitseerijate osakaalud valimiste lõikes

Valimised	E-hääletajate osakaal kõigist osalenud hääletanutest (%)	Verifitseerijate osakaal kõigist e-hääletanutest (%)
KOV 2005	1,9	-
RK 2007	5,5	-
EP 2009	14,7	-
KOV 2009	15,8	-
RK 2011	24,3	-
KOV 2013	21,2	3,4
EP 2014	31,3	4,0
RK 2015	30,5	4,3
KOV 2017	31,7	4,0
RK 2019	43,8	5,3
EP 2019	46,7	4,1

Allikas: Elektroonilise hääletamise statistika

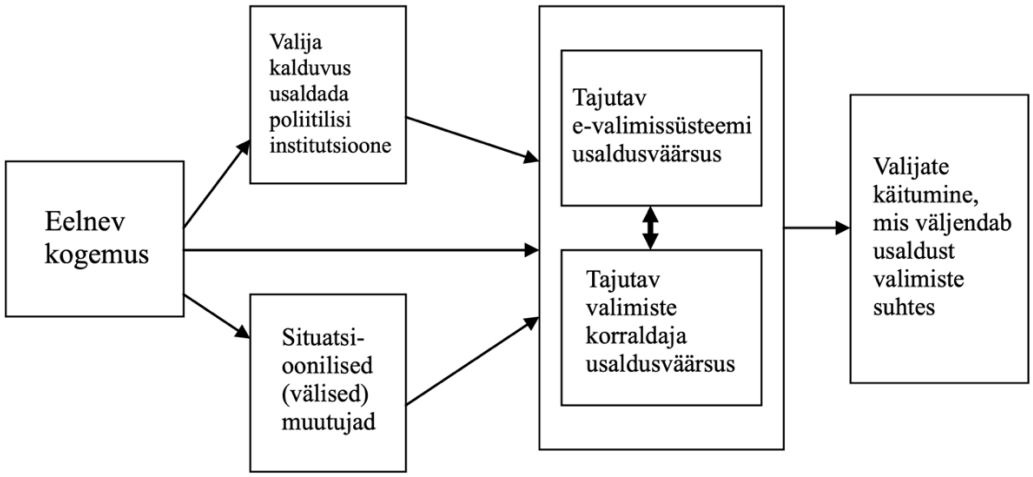
1.3 Verifitseerimine ja usaldus

On ilmne, et demokraatlike ja läbipaistvate valimiste korraldamine on võimalik ainult siis, kui valijad usaldavad valimissüsteemi, usalduse tekitamine on võtmeelement valimistulemuste legitiimsuses (Solvak & Vassil 2016: 128). Inimene hääletab, et arvamust avaldada, aga kui ta ei saa usaldada, et tema arvamust võetakse arvesse, tundub hääletamine mõttetu (Warkentin et al. 2018: 198-199). Valija kui süsteemi kasutaja peab olema täielikult veendunud, et süsteemiga ei saa manipuleerida, et valimiste organisaatorid järgivad eeskirju ning opereerivad süsteemi korrektselt ja süsteemi tulemus peegeldab valija tegelikku valikut (Solvak & Vassil 2016: 49). Olgugi, et Eestis otsustati verifitseerimine implementeerida eelkõige süsteemirünnete tuvastamiseks (Solvak & Vassil 2016: 127), on see algusest peale täitnud ka valija usaldusetaseme tõstmise ülesannet. Individuaalse hääle verifitseerimise võimalus annab valijale lisakindlust, et hääl jõudis kohale, ning kindlustab, et muidu varjatud virtuaalne hääletusprotsess toimib nii, nagu peab (Solvak & Vassil 2016: 128). Sellest tulenevalt peaks verifitseerimist kasutanud e-hääletajate usaldustase tõusma (*Ibid*.), sest valija saab veenduda, et süsteem esindab tema tegelikku valikut.

Verifitseerimise ja usalduse vahelist seost on kolme valimisjärgse küsitluse ja ühe enne ja pärast 2014. aasta Euroopa Parlamendi valimisi läbi viidud paneeluuringu põhjal uurinud Solvak ja Vassil (2016: 127-141). Enne ja pärast valimisi tehtud küsitlus võimaldas võrrelda, kas valija usaldus oli peale hääletamist ja verifitseerimist muutunud (Solvak & Vassil 2016: 134). Uuringust selgus, et usalduse tõus oli suhteliselt väike ning see kajastus võrdselt nii verifitseerijate kui ka mitte-verifitseerijate usalduses, mistõttu ei saanud seda muutust verifitseerimisega seostada (*Ibid.*). Samuti selgus, et need, kes verifitseerimist kasutasid, näitasid e-valimiste suhtes juba eos väga kõrget usaldust, mistõttu ei olnud usalduse tõstmiseks lihtsalt enam ruumi (Solvak & Vassil 2016: 135).

Kuna individuaalse hääle verifitseerimine on võrdlemisi uus nähtus ja selle asjakohane kõrvutamine valija usaldust käsitlevate teooriatega praktiliselt puudub, tuleb kõigepealt vaadata, millest sõltub valija usaldus e-valimiste vastu üldiselt ning kuidas see võiks edasi kanduda verifitseerimise konteksti. Kontseptuaalsel tasandil saab usaldust määratleda kui otsust sõltuda kellestki, teades, et sellega kaasneb teatud risk (Bachmann & Zaheer 2006:

236). Sõltuvus seostub positiivsete ootustega ja kindlusega teise osapoole suhtes ning risk negatiivsetega – kõhklus, et usaldamine võib usaldajale tekitada kahju (*Ibid.*). Tajutava usaldusväärsuse tagajärg on käitumine, mis väljendab usaldust (Avgerou 2013: 427). E-valimiste puhul on selliseks käitumiseks valijaskonna kollektiivne valimistulemuste korrektsuse aktsepteerimine, jättes kõrvale tulemuse enda (valija, kelle valitud kandidaat ei osutunud valituks, võib tulemuses olla pettunud, aga ta ei sea kahtluse alla valimiste legitiimsust). Chrisanthi Avgerou e-valimiste konteksti kohandatud variant Herbert W. Kee ja Robert E. Knoxi (1970: 361) kognitiivsest usaldusväärsuse mudelist (Joonis 1.1) näitab, et valija usalduse tekkimises e-valimiste vastu on kesksel kohal kaks komponenti – kui usaldusväärne on tema jaoks valimiste korraldaja ja kui usaldusväärne on e-valimissüsteem ise (Avgerou 2013: 428).



Joonis 1.1: Valija usalduse kujunemine e-valimiste suhtes. Allikas: Avgerou 2013: 428.

Usaldus e-valimiste läbiviimise protseduuri vastu tuleneb peamiselt valija hinnangulisest usaldusväärsusest valimiste korraldaja suhtes (Avgerou 2013: 426) Valijal võib eelnev kogemus e-hääletamisega puududa, samuti taustateadmised e-valimistest, kuid tal on reeglina mingisugused eelarvamused valimiste organisaatorist, mida võivad omakorda mõjutada erinevad välised tegurid nagu poliitilised liikumised ja meedia (*Ibid.*). Valija jaoks sõltub valimiste korraldaja usaldusväärsus tema ajalooliselt välja kujunenud isiklikest eelsoodumusest usaldada teisi, kogu ühiskonda ja võimuorganeid (Avgerou, 2013:424). Seega sõltub valimiste korraldaja usaldusväärsus osalisel määral valija individuaalsest taustast – kas ta usaldab avalikke institutsioone, võimulolijat, teisi kodanikke. E-hääletaja saab valimisi usaldada siis, kui valimisi korraldav institutsioon on

tema jaoks usaldusväärne. Teinekord piisab valijale institutsiooni usaldamiseks ka üldisest teadmisest, et institutsioonil on hea maine. (Solvak & Vassil 2016: 133).

Teine komponent on e-valimissüsteemi enda usaldusväärsus. Oluline tegur, mis mõjutab inimese otsust e-hääletada, on tema eelarvamused tehnoloogia, igasuguste interneti-transaktsioonide ja elektroonilise hääletamise praktika suhtes (Solvak & Vassil 2016: 63). McKnight et al. (2011: 12) uuring näitas, et üldine tehnoloogia usaldamine on tugevalt seotud konkreetsete tehnoloogiate usaldamisega. Inimene, kellel on üldiselt tehnoloogia suhtes kõrgem usaldus, usaldab suurema tõenäosusega ka mingit spetsiifilist tehnoloogiat, kui tal puudub põhjus seda mitte usaldada (McKnight et al. 2011: 6). E-valimised on olemuselt tehnoloogiline innovatsioon, mille töökindlus sõltub mitmetest tarkvaralistest lahendustest ja mehhaanilistest vahenditest (Avgerou 2013: 426). See tähendab, et usaldada e-valimisi, peaks valija kõigepealt usaldama tehnoloogiat, internetti, hääletamismasinaid ja kaudselt kõiki organisatsioone ja indiviidide, kes nende eest vastutavad (*Ibid.*). Kui inimene usaldab mingit spetsiifilist tehnoloogiat, on suurem tõenäosus, et ta proovib hiljem ka teisi selle tehnoloogia osasid (McKnight et al. 2011: 15). Järelikult, et usaldada verifitseerimist, on kõigepealt tarvilik usaldada elektroonilist hääletamist ning tehnoloogiat üldiselt. Inimene, kelle eelarvamused tehnoloogia ja e-valimiste suhtes on positiivsed, on tõenäoliselt altim verifitseerimist kasutama kui inimene, kes kahtleb kogu domeenis.

E-valimiste usaldusväärsus sõltub valija jaoks seega selle komponentide, valimiste korraldaja ja e-valimissüsteemi, usaldusväärsusest. Seosest on tuletatav, et verifitseerimise usaldamiseks on järelikult tarvilik usaldada e-valimisi, sest verifitseerimise legitiimsus tuletub valija jaoks e-valimiste legitiimsusest. Sellist paradoksaalset nähtust, kus verifitseerivad need, kes süsteemi juba niigi usaldavad, näitas ka Solvaku ja Vassili uuring (Solvak & Vassil 2016: 140). Seega võib teooria põhjal eeldada, et verifitseerimist kasutab valija, kes kaldub juba eos tehnoloogiat, e-valimisi ja valimisi korraldavat institutsiooni usaldama. Vastupidiselt, kui valijal eelmainitud komponentide suhtes usaldust napib, ei ole tal põhjust verifitseerimist kasutada, sest ta tajub ka seda ebausaldusväärsena.

1.4 Verifitseerimise difusioon ühiskonnas

Eelnevas peatükis selgus, et verifitseerimine tõotab olla populaarsem nende seas, kes e-valimisi, poliitilisi institutsioone ja tehnoloogiat usaldavad. See aga ei paku ammendavat vastust küsimusele, kas verifitseerimine ise valija usaldust tõstab. Kuna uurimuse aluseks olevates küsitlustes paluti valijal hinnata oma usaldust ühekordselt peale igat valimist, ei ole kahjuks võimalik puhtempiiriliselt seletada, kuidas on valija usaldus muutunud vahetult enne ja pärast valimisi. Küsitlusandmed ei seleta, kas valija usaldus oli juba enne valimisi kõrge või tõusis see konkreetselt tänu verifitseerimisele. Järgnevas alapeatükis täiendatakse verifitseerimise ja usalduse vahelise interaktsiooni seletust, toetudes verifitseerimisrakenduse levikule ühiskonnas, mis viitab sellele, kes rakendust parasjagu kasutavad. Kui kasutajad moodustavad mingi spetsiifilise sotsio-demograafilise grupi, võib neile iseloomulike tunnuste põhjal oletada, mis motiveerib neid häält verifitseerima ning millist mõju see nende usaldustasemele avaldab. Eeskujuks võetakse varasemad käsitlused e-hääletamise difusioonist ühiskonnas ning lähtutakse eeldusest, et kuna verifitseerimine on oma olemuselt üks funktsionaalne komponent e-valimissüsteemist, on selle kasutajaskond sisuliselt üks kitsam ja spetsiifilisem alamhulk kogu e-valijaskonnast.

Solvak ja Vassil (2016: 59-70) toetuvad e-hääletamise difusiooni kirjeldamisel Everett M. Rogersi (2003) tehnoloogilise difusiooni teooriale, mis kirjeldab, kuidas võetakse mingi teatud tehnoloogiline lahendus ajapikku ühiskonnas omaks. Teooria näeb ette, et niinimetatud esimese ringi kasutajad moodustavad üsnagi kitsa ja spetsiifilise grupi – teadlikud ja innovaatilise lähenemisega kasutajad, kes on valmis riskima ning uue tõestamata innovatsiooni proovile panema. (Solvak & Vassil 2016: 60). Kui selle grupi kogemus innovatsiooniga on positiivne, hakkab tehnoloogia difuseeruma (Vassil et al. 2016: 454). Iga järgneva ringiga liituvad uue tehnoloogia kasutajaskonnaga inimesed, kes sarnanevad varajastele adopteerijatele üha vähem, kuni difusiooni lõpustaadiumis jõuavad järgi ka need, kes uue tehnoloogia proovimisest esialgu üldse huvitatud ei olnud (Solvak & Vassil 2016: 60). E-hääletajad peaks selle teooria järgi ajapikku paberhääletajatega sarnastuma, sest neile algselt iseloomulikud tunnused hakkavad aja möödudes oma tähtsust kaotama (Solvak & Vassil 2016: 62). Vassil et al. uuring (2016: 458) näitas, et e-hääletamise puhul avaldus difusiooni kulgemine platooefektina peale kolme valimist. Mitmed e-valijale iseloomulikud tunnused hakkasid seejärel tõepoolest

oma mõju kaotama (Vassil et al. 2016: 456-457), mis tähendab, et e-hääletamine hakkas efektiivselt laiema valijaskonna seas levima.

Reeglina vastab eelmainitud varajaste adopteerijate grupp teatud sotsio-demograafilisele profiilile, millest võivad kohati sõltuda ka nende hoiakud (Solvak & Vassil 2016: 60). E-hääletamise puhul oli selleks grupiks nooremapoolsed (kuni 40-50 aastased) eestlased (Solvak & Vassil 2016: 64-65), keda iseloomustas hea arvutikasutusoskus ja kõrge usaldus e-valimiste vastu (Vassil et al. 2016: 458). Verifitseerimise asetamisel tehnoloogilise difusiooni konteksti lähtutakse Solvaku ja Vassili (2016: 141) järeldusest, et verifitseerimist esimesena proovinud e-hääletajad on alamhulk nendest samadest innovaatilise lähenemisega inimestest, kes katsetasid esimesena ka e-hääletamist, kui see toona kasutusele võeti. Rogersi tehnoloogilise difusiooni teooria kohaselt sõltub see, kas ja kui kiiresti leiab difusioon ühiskonnas aset, viiest omadusest (Rogers 2003: 79), mille abil seletatakse järgnevalt verifitseerimisrakenduse potentsiaali hakata levima laiema valijaskonna seas.

Suhteline eelis – kui palju tajutakse innovatsiooni eelist selle idee või tegevuse ees, mida see asendama peaks (Rogers 2003: 77). Mida paremini tajutav on suhteline eelis, seda kiiremini võetakse innovatsioon omaks (*Ibid.*). Verifitseerimine püüab asendada seda momenti konventsionaalse paberhääletamise protsessis, kus valijal on võimalus veenduda selles, et ta presenteerib oma valikut korrektselt - paber ja pliiats on kasutatavad, ning ta saab sedeli isiklikult kabiinist valimiskastini viia (Heiberg & Willemson 2014: 2). Verifitseerimise eeliseks peaks siinkohal olema mugavus ja lihtsus, mis on ühtlasi ka üldiselt aktsepteeritud e-valimiste eelis paberhääletamise ees. Tuleb aga arvestada, et hääle kontrollimine on valija jaoks kõigest üks vabatahtlik osa hääletamise protsessist. Valija, kes peab hääle kontrollimist (ka paberhääletamise puhul) ebaoluliseks, verifitseerimises tõenäoliselt suurt eelist ei näe.

Sobivus – kui palju tajutakse, et innovatsioon sobitub inimeste väärtuste, vajaduste ja varasemate kogemustega (Rogers 2003: 77). Ideid, mis ei sobitu ühiskonna normidega, ei võeta vastu sama kiirelt kui neid, mis sobituvad (*Ibid.*). Hääle verifitseerimine ei ole nii mõnegi valija jaoks kaugeltki niivõrd oluline ja vajalik protseduur kui hääletamine ise. Paljud valijad ei pea verifitseerimist vajalikuks, sest nad ei ole riskidest, veel vähem süsteemirünnete võimalikkusest teadlikud (Kulyk & Volkamer 2018: 70). Leidub ka neid, kes on riskidest teadlikud, kuid nad ei muretse oma hääle terviklikkuse pärast, sest

tõenäosus, et nad rünnaku ohvriks satuvad, on väike (Kulyk & Volkamer 2018: 70-71). Võimalik, et mõni hääletaja tunneb sotsiaalsest survest tulenevalt sootuks, et ta paistab verifitseerides paranoiline (Kulyk & Volkamer 2018: 72) ning jätab seetõttu verifitseerimata. Kõik eelmainitu vähendab tõenäosust, et valija kasutab verifitseerimist (Kulyk & Volkamer 2018: 70-73). Teisalt võib verifitseerimine valija kahtluste leevendamise asemel neid hoopis süvendada. Kuigi verifitseerimise eesmärk on süsteemi läbipaistvuse tõstmine, ei pruugi see valija jaoks alati nii paista. Keskmine e-valija, kes ei ole tõenäoliselt verifitseerimise tehnilise poolega kursis, võib kahtlema hakata näiteks süsteemi anonüümsuses. Kas keegi teine näeb ka minu häält, kas süsteem ei olegi anonüümne? Miks ma pean üldse häält kontrollima, kas süsteem ei olegi turvaline? Näeme, et verifitseerimise sobivus inimeste vajaduste ja väärtustega võib difusiooni kulgemisel arvestatavaks pudelikaelaks osutuda.

Keerukus – kergesti hoomatav lahendus võetakse kiiremini vastu kui lahendus, mis nõuab kasutajalt konkreetseid oskusi või teadmisi (Rogers 2003: 78). Verifitseerimise kasutajate nappuses on sageli süüdlaseks peetud selle protseduurilist keerukust (Kulyk & Volkamer 2018: 66-67). Kuna verifitseerimiseks on loomulikult tarvilik, et valija on juba edukalt e-hääletanud, siis tõenäoliselt on tema arvutikasutusoskus ka verifitseerimiseks piisav. Siiski võib Eesti süsteemi keerukust tõsta asjaolu, et erinevalt e-hääletamisest on verifitseerimiseks vajalik ligipääs kaamera ja internetiühendusega nutiseadmele ning oskus kasutada QR-koodi (E-hääle kontrollimine). Kui need tingimused ei ole täidetud, tähendab see automaatselt, et valija ei saa rakendust kasutada, isegi, kui ta on sellest teadlik ja tema suhtumine soosib verifitseerimist. See kitsendab potentsiaalsete kasutajate hulka veelgi.

Katsetatavus[3] – lahendus, mida saab eelnevalt järgi proovida, võetakse üldiselt omaks kiiremini kui lahendus, mida ei saa proovida (Rogers 2003: 78). Erinevalt e-valimistest, kus enamikel juhtudel saavad valijad enne valimisi proovida, kuidas süsteem töötab (Solvak & Vassil 2016: 52), ei saa e-hääletajad valimiste eel proovida verifitseerimist. Verifitseerimise selgeks eelduseks on, et kõigepealt on süsteemile edastatud hääl, mida saaks verifitseerida – seetõttu ei saa hääletajale enne valimisi pakkuda e-hääletamisega

[3] Ing k. *trialability*

samaväärset simulatsiooni, küll aga on Eesti valimiste kodulehel ekraanipiltidega illustreeritud juhend hääle kontrollimiseks (E-hääle kontrollimine).

Jälgitavus[4] – Kui innovatsiooni tulemus on kõrvalt vaatajaile selge ja nähtav, siis on ka suurem tõenäosus, et nad võtavad selle kiiresti omaks (Rogers 2003: 79). Verifitseerimise tulemuseks on valijaskonna kollektiivne veendumus süsteemi terviklikkuses ja läbipaistvuses. Kuna kasvõi ühe verifitseerija positiivsest tulemusest peegeldub, et süsteem loeb hääli korrektselt, saab ka ülejäänud valijaskond süsteemi rohkem usaldada. Solvaku ja Vassili (2016: 137-138) uuring näitas samuti, et usalduse jaotused verifitseerimist kasutanud e-hääletajate ja nende vahel, kes selle olemasolust ainult teadsid, ei erinenud oluliselt, verifitseerijatel oli lihtsalt natuke kõrgem keskmine usaldustase. Mõnele valijale piisab teadmisest, et häält saab kontrollida ja teiste hääled läksid korrektselt arvesse. Kõrvalt vaadeldavus võib seega verifitseerimise puhul osutuda oluliseks difusiooni pidurdavaks teguriks, sest valija, kellele piisab teiste positiivsetest tulemusest, ei tunne vajadust ise verifitseerimist kasutada.

Näeme, et nii mõnegi omaduse puhul avaldusid selged kitsaskohad, mistõttu ei ole verifitseerimine Rogersi tehnoloogilise difusiooni teooria kohaselt eriti hästi leviv innovatsioon. Difusioon tõotab ühiskonnas kulgeda aeglaselt – verifitseerimist ei võeta piisavalt kiiresti omaks ning varajastele adopteerijatele iseloomulikud tunnused kaotavad mõju aeglaselt või ei kaota üldse, sest uusi adopteerijaid on vähe. Selle põhjal võib eeldada, et verifitseerijate grupp on jätkuvalt üsna spetsiifilise taustaga ja keskmisest e-valijast eristuv muuhulgas kõrgema arvutioskuse ja usalduse poolest. Sellest tuleneb, et valija usaldustase ei sõltu niivõrd verifitseerimisest, pigem vastupidi – verifitseerib valija, kes kaldub juba niigi e-valimisi usaldama, sest talle on iseloomulikud tunnused, mis verifitseerimist soodustavad (kõrge arvutikasutusoskus, tendents usaldada valimisi, poliitilisi institutsioone ja tehnoloogiat). Teooria viitab sellele, et verifitseerimise haare ühiskonnas ning efekt valija usalduse suhtes ei ole Solvaku ja Vassili uuringust saati oluliselt muutunud ning rakendus on kokkuvõttes endiselt nišistaatuses.

[4] Ing k. *observability*

2 Uurimisobjektid

2.1 Uurimuse eesmärk

Eelmises peatükis selgus, et Eestis 2013. aastal implementeeritud individuaalse hääle verifitseerimise üks eesmärkidest on tõsta valija usaldust kogu e-valimissüsteemi vastu. Samas selgus, et verifitseerimise kasutajaskond koosneb enamasti suhteliselt spetsiifilise taustaga inimestest, kelle usaldus e-valimiste vastu tõotab olla niigi kõrge. Samuti selgus, et valija usaldustaset võib mõjutada ka pelgalt verifitseerimisest teadmine. Käesoleva töö fookus on empiiriliste andmete põhjal kontrollida, kas ja mil määral on verifitseerimise võimalus valija usaldust tegelikult mõjutanud. Lisaks uuritakse, kas teoorias tüüpilisele verifitseerijale iseloomulikud tunnused avalduvad päriselt e-hääletajate seas ning kas nende tunnuste mõju on ajas kahanenud, ehk kas rakendus on laiema kasutajaskonna seas levima hakanud.

2.2 Uurimisküsimused ja hüpoteesid

K1. Kuidas erineb verifitseerimist kasutanud e-hääletajate usaldus a) verifitseerimisest teadlike usaldusest b) verifitseerimisest mitteteadlike usaldusest?

K2. Kuidas on e-valijaskonna usaldustase peale verifitseerimise võimaluse lisandumist muutunud?

K3. Millised tunnused iseloomustavad „tüüpilist verifitseerijat“ ning kas nende mõju verifitseerimise tõenäosusele on viimase kuue valimise jooksul muutunud?

H1. Nende usaldus, kes verifitseerimisest teadsid, on kõrgem kui nende usaldus, kes verifitseerimisest ei teadnud. Verifitseerimist päriselt kasutanud e-hääletajate usaldus on omakorda pisut kõrgem, kui teadlike usaldus.

H2. E-valijaskonna usaldustasemes muutus ei kajastu, sest verifitseerimist kasutab väga väike hulk e-valijaid, kelle usaldustase kipub niigi kõrge olema.

H3. Tüüpiline verifitseerija sarnaneb algsele tüüpilisele e-valijale: nooremapoolne keskmisest parema arvutikasutusoskusega eestlane, kellel on e-valimiste suhtes kõrge usaldus. Tunnuste olulisus ei ole ajapikku kahanenud, sest verifitseerimise difusioon kulgeb aeglaselt või ei kulge üldse.

3 Metoodika

3.1 Valim

Käesolevas uurimuses teostatud andmeanalüüs baseerub Johan Skytte poliitikauuringute instituudi poolt läbi viidaval läbilõikelisel valimisjärgsel küsitlusuuringul. 2005-2019 aastal läbi viidud uuringust kasutatakse antud uurimuses enamasti küsitlusandmeid perioodist, mil verifitseerimist kasutati (2013-2019). 2013. aastast alates kasutati küsitlustes stratifitseeritud juhuvalimit, küsitletavate arvu suurusjärgud olid iga küsitluse puhul võrreldavad (täpne arv jäi vahemikku 1000-1042 vastajat). Kokku on analüüsi aluseks ligi 6000 intervjuuga andmestik.

Andmeanalüüsi esimeses pooles vaadeldakse verifitseerimise mõju valija usaldust näitavatele tunnustele. Enamasti eristatakse kolme gruppi: verifitseerimist kasutanud e-hääletajad, verifitseerimisest teadlikud e-hääletajad ja verifitseerimisest mitteteadlikud e-hääletajad. Sellest tulenevalt on sõltumatuteks tunnusteks verifitseerimine ja verifitseerimisest teadmine. Sõltuvateks tunnusteks on:

a) **Usaldus e-valimiste vastu** – vastajal paluti hinnata oma usaldust e-valimissüsteemi vastu skaalal 0-10, kus 0 tähistab usalduse puudumist ja 10 täielikku usaldust.
b) **Usaldus, kas valija enda hääl läks arvesse** – vastajal paluti hinnata, kui palju nad usuvad seda, et nende hääl läks e-valimistel arvesse, skaalal 1-4, kus 1 tähistab usalduse puudumist ja 4 täielikku usaldust.
c) **Usaldus, kas teiste hääled läksid arvesse** – vastajal paluti hinnata, kui palju nad usuvad seda, et teiste valijate hääled läksid e-valimistel arvesse, skaalal 1-4, kus 1 tähistab usalduse puudumist ja 4 täielikku usaldust.

Andmeanalüüsi teises pooles vaadeldakse erinevate sotsio-demograafiliste ja digipädevust väljendavate tegurite mõju verifitseerimise tõenäosusele. Regressioonanalüüsi sõltuv muutuja oli alati binaarne – verifitseeris või mitte. Sõltumatuteks muutujateks valiti need tunnused, mis Solvaku ja Vassili (2016: 59-70) uuringu põhjal algselt e-hääletajaid paberhääletajatest eristasid. Lisati ka QR-koodi kasutamise kogemus. See ei ole verifitseerimiseks tarvilik, sest verifitseerida saab ka ilma eelneva kogemuseta, aga see ilmestab teatud määral inimese aruvuti kasutamise oskust. Seevastu

otsustati mitte kaasata nutiseadme olemasolu tunnust, sest kuna nutiseade on verifitseerimiseks selgelt tarvilik, on mõju verifitseerimise tõenäosusele ilmne.

d) **Vanus**
e) **Sugu**
f) **Emakeel** (rahvus) – analüüsis eristati ainult eesti- ja venekeelseid e-valijaid. Muu emakeelega vastajaid oli küsitluses marginaalselt, ning tulenevalt sellest, et analüüs baseerub juba niigi kitsal alamhulgal, ei näidanud teised keeled tehtud mudelites mitte mingit statistilist olulisust.
g) **Enesehinnanguline arvutikasutusoskus** – vastajal paluti hinnata oma arvutioskust skaalal 0-4, kus 0 tähistab oskuse puudumist ja 4 väga head arvutioskust.
h) **QR-koodi kasutamise kogemus** – vastajal paluti hinnata oma kogemust QR-koodi kasutamisega skaalal 1-4, kus 1 tähistab QR-koodist üldse mitte teadmist ning 4 sagedast QR-koodi kasutamist.

3.2 Andmeanalüüsi meetod

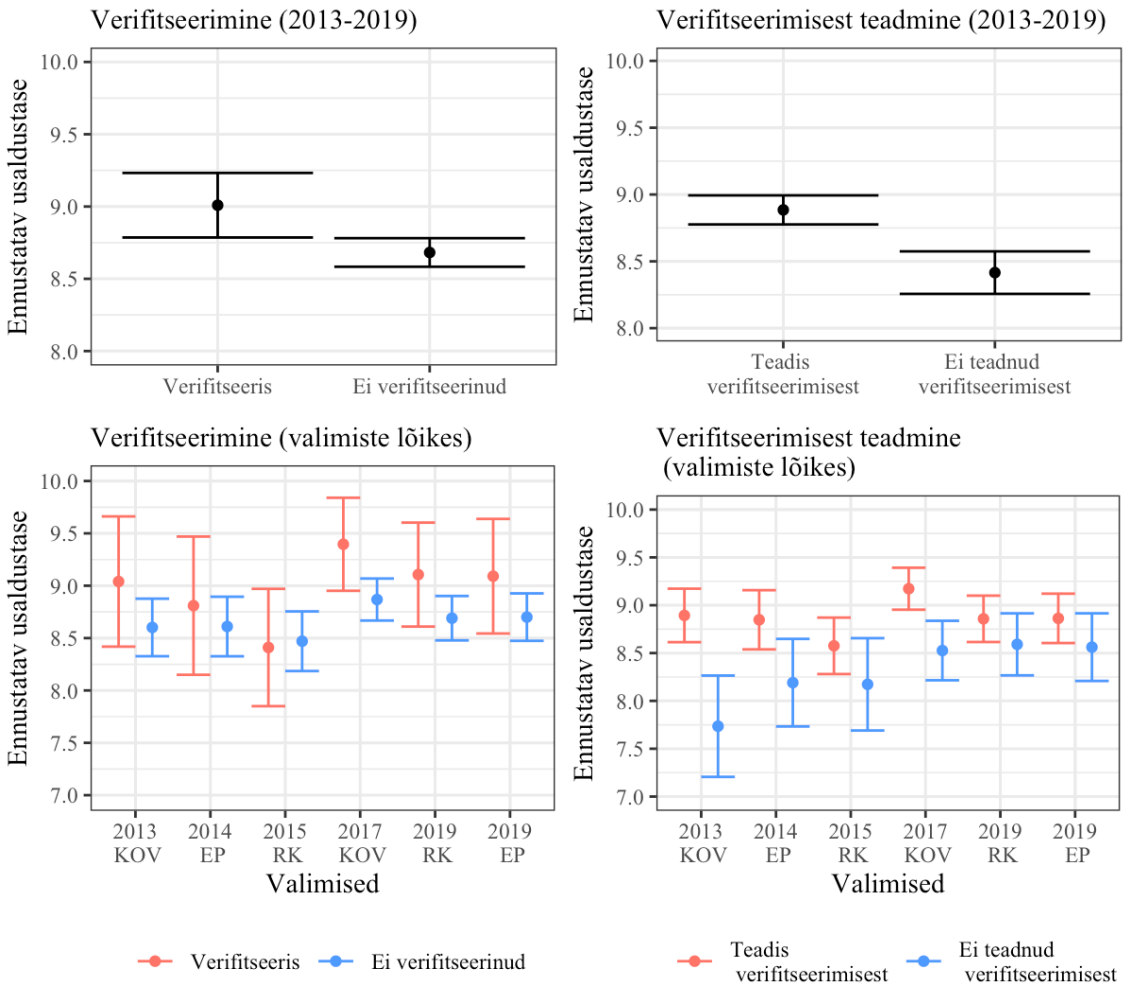
Küsitlusandmete kvantitatiivseks analüüsiks kasutati vabavaralist andmetöötluspaketti RStudio (versioon 1.2.5). Seoste modelleerimisel kasutati logistilist regressiooni. Valik üldistatud lineaarse mudeli kasuks tulenes sellest, et vähemalt üks tunnus osutus alati binaarseks (verifitseeris või ei verifitseerinud, teadis verifitseerimisest või ei teadnud) ning teine tunnus oli kas binaarne või normaaljaotuslik, olenevalt sellest, mida see tunnus parasjagu representeeris. Seose statistilist olulisust hinnati regressioonimudeli p-väärtuse järgi. Seos loeti statistiliselt oluliseks, kui kehtis $p \leq 0,05$.

Kasutajabaasi uurimisel vaadeldi konkreetselt seda, kuidas mõjutavad valitud tunnused verifitseerimise kasutamise tõenäosust. Seetõttu eelistati regressioonanalüüse läbi viia nende valijate hulgaga, kes olid verifitseerimise olemasolust üldse teadlikud. Verifitseerimisest teadlike hulk oli aga võrdlemisi marginaalne ning paraku osutus valija usaldust näitavate tunnuste puhul vajalikuks laiendada vaatlusalust gruppi kõigi e-hääletajateni, sest verifitseerimisest teadjate hulgaga tehtud analüüs ei pakkunud järelduste tegemiseks piisavalt selgeid tulemusi. Nendel juhtudel arvestati, et e-hääletaja ei kasutanud verifitseerimist, kuigi ta ei olnud sellest tegelikult isegi teadlik.

4 Andmeanalüüs

Perioodil 2013-2019 hääletas interneti teel 1449 küsitlusele vastajat. Neist 945 vastajat teadsid ja 444 vastajat ei teadnud verifitseerimise olemasolust. Verifitseerimisest teadlike hulgas omakorda kasutas verifitseerimist 225 inimest ning ei kasutanud 710 inimest. Ebakõla hulkade summeerimisel tekib mõlemal juhul sellest, et ülejäänud vastajad kas ei osanud või ei soovinud küsimusele vastata.

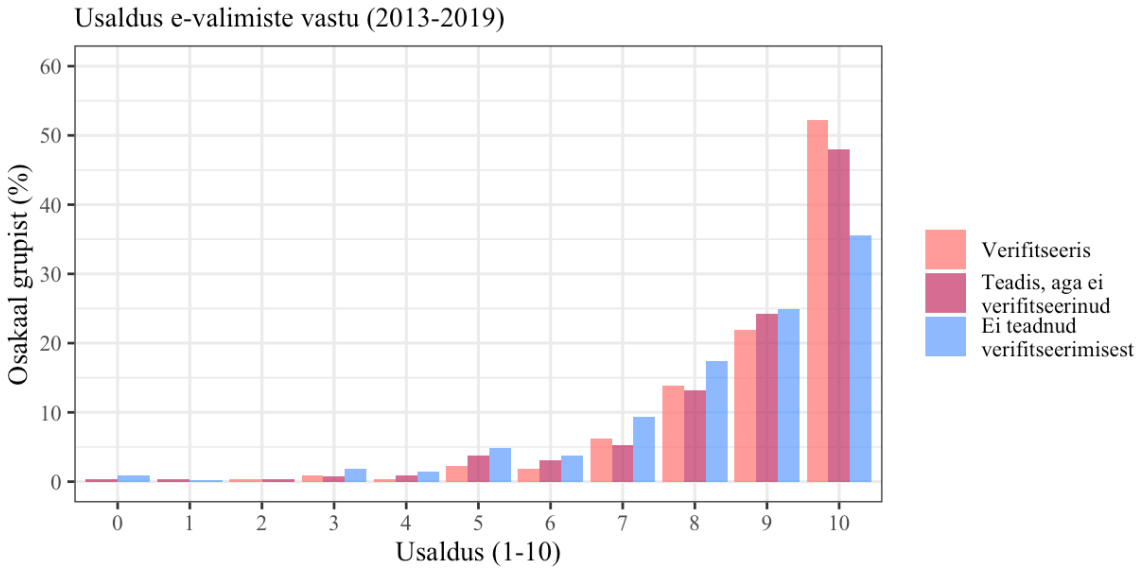
4.1 Verifitseerimise mõju usaldusele



Joonis 4.1: verifitseerimise ja verifitseerimisest teadmise efekt usaldusele (kõik e-hääletajad, 2013-2019)

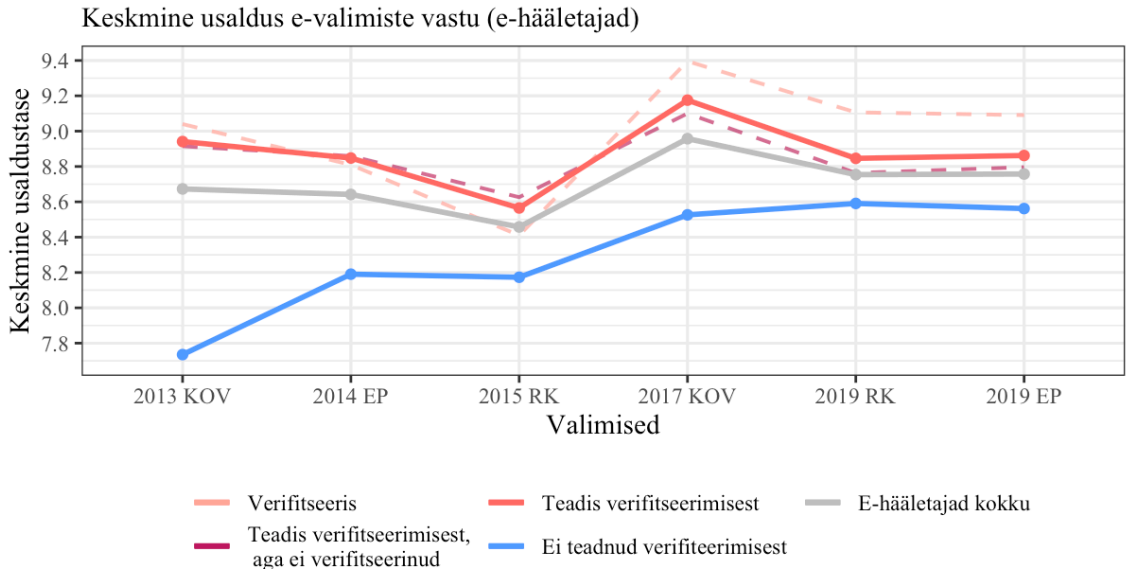
Esmalt uuriti verifitseerimise seost sellega, kui palju valija e-valimissüsteemi usaldab. Sõltuv tunnus oli usaldus ja sõltumatu tunnus verifitseerimine. Verifitseerimisest teadlike grupiga läbi viidud logistiline regressioon näitas, et see, kas valija päriselt ka verifitseeris, usaldustasemele statistiliselt olulist mõju ei avaldanud ($p \geq 0,05$). Efekt avaldus alles siis, kui vaatlusaluseks grupiks võeti kõik e-hääletajad, sealhulgas need, kes ei olnud verifitseerimise olemasolust teadlikud (Joonis 4.1). Verifitseerijate ennustatav usaldustase oli siis mitte-verifitseerijate omast keskmiselt 3,8% kõrgem. Kui kogu perioodi hõlmavas mudelis oli efekt statistiliselt oluline, siis valimiste lõikes avaldas verifitseerimine usaldusele mõju vaid 2017. aasta KOV valimistel. Seetõttu ei efekti olulisuse muutust ajas tähendada.

Mõnevõrra suuremat mõju avaldas verifitseerimisest teadmine – kõigi e-hääletajate seas teostatud logistiline regressioon näitas, et verifitseerimisest teadjate ennustatav usaldustase oli mitte-teadjate omast keskmiselt 5,6% kõrgem. Samuti avaldas verifitseerimisest teadmine usaldusele kohati mõju valimiste lõikes – verifitseerimisest teadmise efekt oli oluline 2013. ja 2017. aasta KOV valimistel ning 2014. aasta Euroopa Parlamendi (EP) valimistel. 2015. aasta Riigikogu (RK) valimistel ning 2019. aasta RK ja EP valimistel efekt enam usaldusele statistiliselt olulist mõju ei avaldanud ($p \geq 0,05$), ehk verifitseerimisest teadmise mõju valija usaldustasemele on ajapikku kahanenud ning lõpuks olulisuse kaotanud.



Joonis 4.2: Usalduse jaotus kolmes grupis (verifitseerimine ja sellest teadmine, 2013-2019)

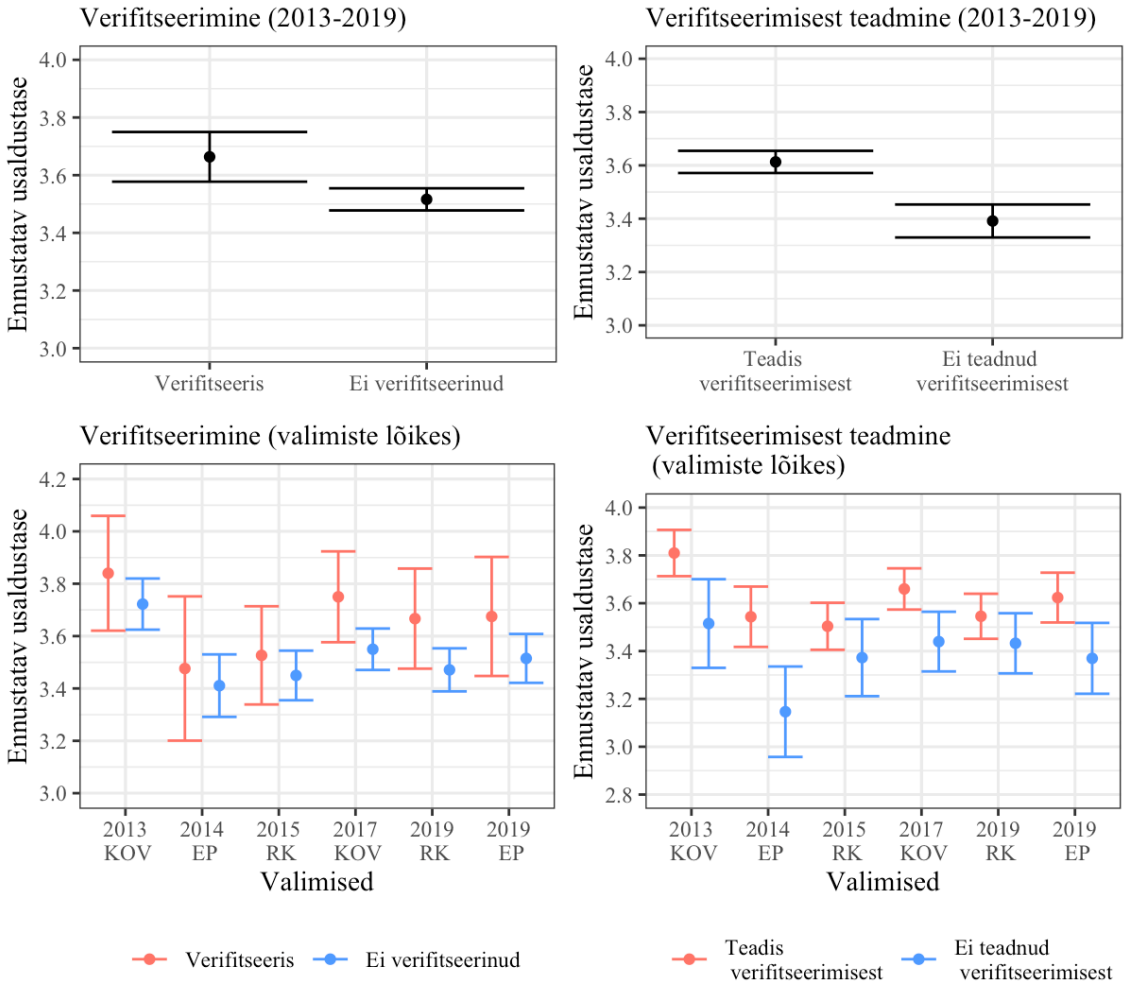
Joonisel 4.2 on kujutatud e-hääletajate usalduse protsentuaalset jaotust kolmes grupis – verifitseerimist kasutanud e-hääletajad, verifitseerimisest teadnud e-hääletajad ja verifitseerimisest mitte teadnud e-hääletajad. Valijad, kes kasutasid verifitseerimist või olid verifitseerimisest teadlikud hindasid oma usaldust kõrgemalt, kui need, kes verifitseerimisest ei teadnud. Näeme, et verifitseerijate ning verifitseerimisest teadjate osakaalud olid märkimisväärselt sarnased, mis seletab seda, miks ei olnud see verifitseerimisest teadlike hulgas statistiliselt oluline, kas verifitseerimist ka päriselt kasutati. Verifitseerimisest mitteteadlike jaotus oli ühtlasem, suurim erinevus verifitseerimisest teadlikega avaldus skaala positiivses äärmuses - täielike usaldajate osakaal oli 10-15% võrra väiksem, kui ülejäänud kahe grupi vastav osakaal.



Joonis 4.3: E-hääletajate keskmine usaldus e-valimiste suhtes valimiste lõikes (2013-2019)

Joonisel 4.3 on kujutatud e-hääletajate keskmise usaldustaseme muutus perioodil 2013-2019, jaotatud verifitseerimise ja verifitseerimisest teadmise tunnuse järgi. Näeme, et verifitseerimist kasutanud ja verifitseerimisest teadnud e-hääletajate usaldus perioodi vältel kokkuvõttes oluliselt ei muutunud, teadlike usaldustase koguni langes veidi. Sellegipoolest oli verifitseerimisest teadlike usaldustase stabiilselt kõrgem kui kõigi e-hääletajate keskmine usaldustase. Näeme, et mitteteadlike usaldustase tõusis perioodi vältel stabiilselt – keskmiselt 2,1% iga küsitlusega. Tulemusena vähenes perioodi vältel kontrast verifitseerimisest teadlike ja mitte teadlike valijate usaldustasemete vahel, kuid kogu e-hääletajate usaldus tõusis keskmiselt vaid 0,2%, ehk olulist muutust valija üldises usaldustasemes tähendada ei saa. Aastatel 2005-2011 langes usaldus iga küsitlusega

keskmiselt 0,58% kuid küsitluses kasutati kitsamat skaalat, mistõttu ei saa neid perioode omavahel hästi võrrelda. See illustreerib pelgalt asjaolu, et valija keskmine usaldustase ajapikku olulisel määral muutunud ei olegi.

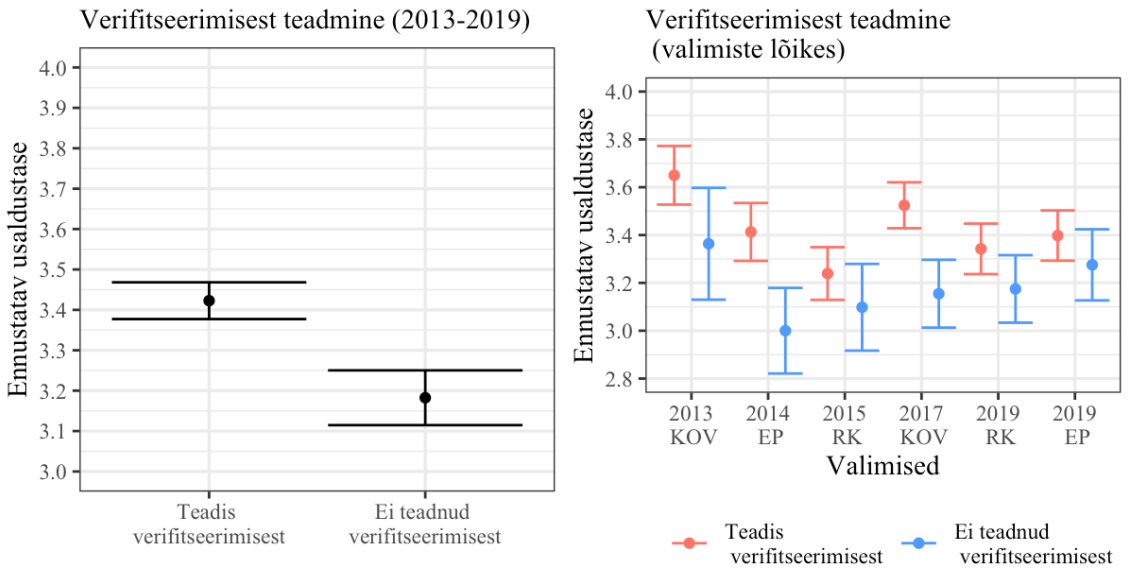


Joonis 4.4: verifitseerimise ja verifitseerimisest teadmise mõju usaldusele, kas valija enda hääl läks arvesse (kõik e-hääletajad, 2013-2019)

Järgnevalt võeti sõltuvaks tunnuseks valija usaldus, kas tema enda hääl läks valimistel arvesse, ehk konkreetselt see, mida verifitseerimine valja enda arvates näitama peaks. Verifitseerimisest teadjate grupi peal tehtud logistiline regressioon näitas jälle, et see, kas valija ka päriselt verifitseerib, ei avaldanud tunnusele statistiliselt olulist mõju ($p \geq 0,05$). Efekt avaldus taas alles siis, kui vaatlusalust gruppi laiendati kõigi e-valijateni, kaasates regressioonimudelisse ka need, kes verifitseerimisest ei teadnud. Joonis 4.4 kujutab verifitseerimise ja verifitseerimisest teadmise mõju sellele, kas e-hääletaja usub, et tema hääl läks valimistel arvesse. Näeme, et verifitseerinud e-hääletajate ennustatav usaldus oli keskmiselt 4,2% kõrgem, nende e-hääletajate omast, kes ei verifitseerinud. Kui kogu

perioodi hõlmav mudel näitas keskmist statistilist olulisust, siis valimiste lõikes oli verifitseerimine nõrgalt statistiliselt oluline vaid 2017. aasta KOV valimistel. Seetõttu ei saa efekti suuruse muutumist ajas adekvaatselt hinnata.

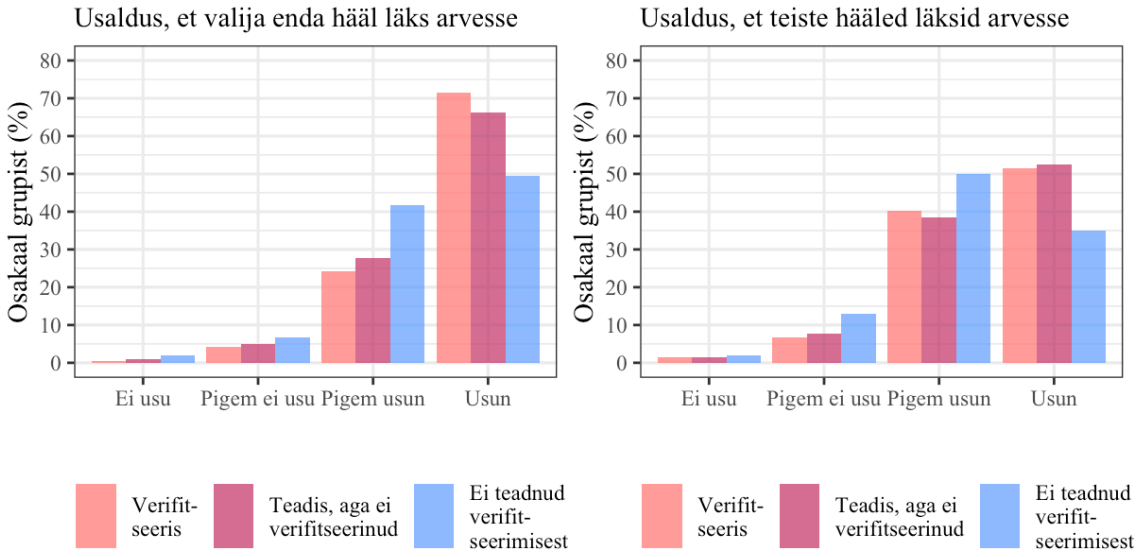
Nagu üldise usaldustaseme puhul, oli ka selle tunnuse puhul verifitseerimisest teadmise mõju kogu perioodi vältel suurem, kui verifitseerimise enda mõju. Verifitseerimisest teadjate ennustatav usaldus hääle arvesse võtmise suhtes oli keskmiselt 6,5% kõrgem nende omast, kes verifitseerimisest ei teadnud. Valimiste lõikes oli verifitseerimisest teadmise mõju statistiliselt oluline 2013 ja 2017 KOV valimistel ning 2014 ja 2019 EP valimistel. Efekti muutuse tõlgendamist raskendavad suured usaldusvahemikud, aga esimesel kahel valimisel oli efekt selgelt suurem kui ülejäänud valimistel. Seetõttu võib järeldada, et verifitseerimisest teadmise mõju hääle usaldusele, kas valija hääl läks arvesse, on mingil määral kahanenud. Muuhulgas näeme huvitavat mustrit – efekti mõju on olnud statistiliselt olematu mõlematel Riigikogu valimistel ning oluline KOV ja EP valimistel.



Joonis 4.5: verifitseerimisest teadmise mõju usaldusele, kas teiste hääled läksid arvesse (e-hääletajad, 2013-2019)

Kolmandaks sõltuvaks tunnuseks võeti valija usaldus selle suhtes, kas teiste hääled läksid valimistel arvesse. Sellele tunnusele ei avaldanud verifitseerimine statistiliselt olulisel määral mõju mitte ühelgi valimisel eraldi, ega ka terve perioodi vältel kokku. Küll aga mõjutas usaldust taas verifitseerimisest teadmine (Joonis 4.5). Teadlike ennustatav usaldus oli mitteteadlike omast keskmiselt 7,6% kõrgem. Valimiste lõikes oli

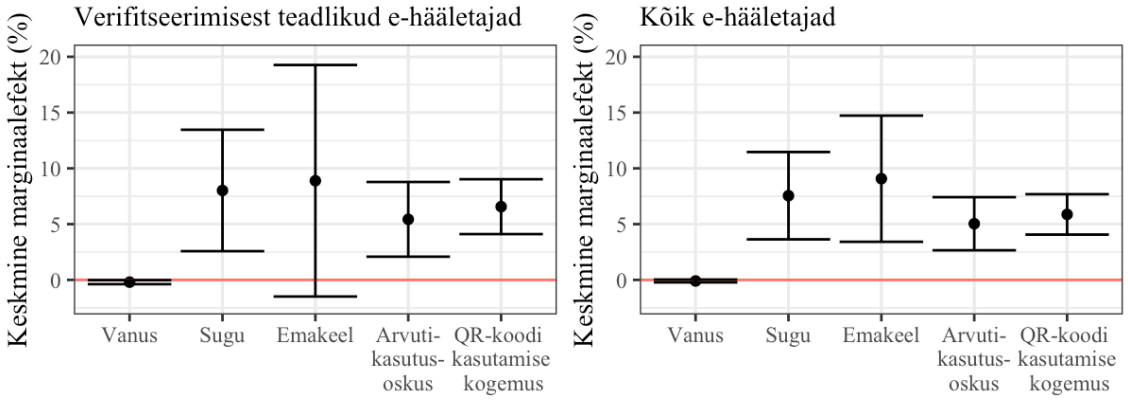
verifitseerimisest teadmine oluline 2013 ja 2017 KOV valimistel ning 2014 EP valimistel. Üldine tendents näitab seega, et verifitseerimisest teadmise mõju usaldusele, kas teiste hääled läksid arvesse, on ajapikku kahanenud.



Joonis 4.6: Usalduse, kas enda ja teiste hääled läksid arvesse, jaotused kolmes grupis (verifitseerimine ja sellest teadmine, 2013-2019)

Joonis 4.6 kujutab jaotusi kolme grupi usaldusest, kas enda ja teiste hääled läksid e-valimistel arvesse. Näeme, et verifitseerimist kasutanud või sellest vähemalt teadnud valijad hindasid oma usaldust märksa kõrgemalt kui need, kes verifitseerimisest ei teadnud. Enda hääle puhul oli mitteteadlike täielike usaldajate osakaal keskmiselt ligi kolmandiku võrra madalam kui ülejäänud kahe grupi vastavad osakaalud. Kolmandiku võrra madalam oli mitteteadlike täielike usaldajate osakaal ka siis, kui vaadeldi valija usaldust teiste valijate häälte suhtes. Näeme, et verifitseerimisest teadnud ja seda päriselt kasutanud e-hääletajate usalduse jaotused on märkimisväärselt sarnased, ehk taas paistab, et verifitseerimise kasutamine usaldust oluliselt ei mõjuta. Huvitav on tähendada, et jaotused olid teiste hääle arvesse võtmise puhul märgatavalt ühtlasemad, ehk inimene kipub millegipärast rohkem uskuma, et tema häälega on kõik korras kui et teiste häältega on kõik korras.

4.2 Tunnuste mõju verifitseerimise tõenäosusele



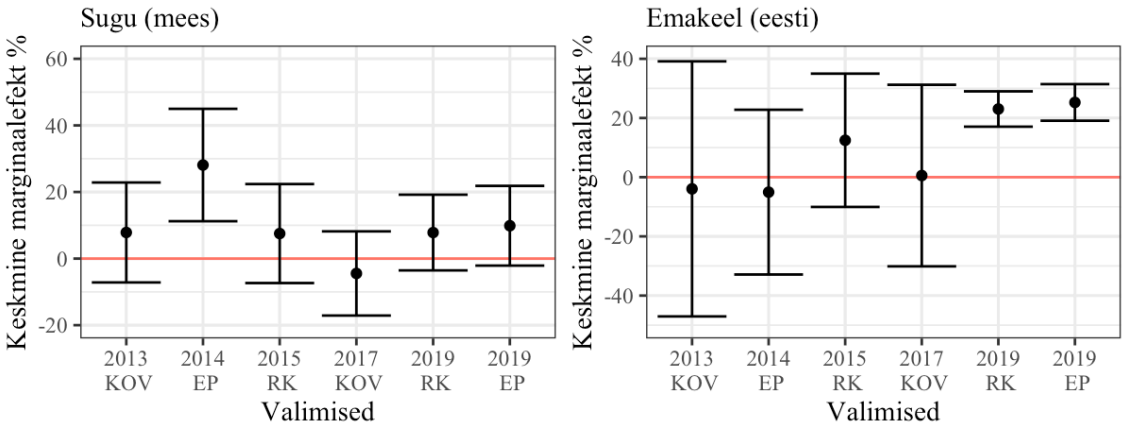
Joonis 4.7: sotsio-demograafiliste ja digipädevust näitavate tegurite mõju verifitseerimise tõenäosusuele (2013-2019)

Joonis 4.7 kujutab erinevate sotsio-demograafiliste ja digipädevust väljendavate tunnuste mõju tõenäosusele, kas verifitseerimisest teadlik valija rakendust ka kasutab. Sõltuvaks tunnuseks võeti verifitseerimine ning sõltumatuteks tunnusteks vanus, sugu, emakeel (rahvus), enesehinnanguline arvutikasutusoskus ja eelnev QR-koodi kasutamise kogemus. Regressioonanalüüs viidi läbi iga tunnuse kohta eraldi, kuid efektide suurust visualiseeriti ülevaatlikkuse tagamiseks ühel joonisel. Kuna eesmärgiks oli teada saada, kas valitud tunnused mõjutavad inimese otsust verifitseerida, siis regressioonianalüüse eelistati läbi viia verifitseerimisest teadjate hulgaga. Sellega välistati valijad, kes näiteks oskasid QR-koodi kasutada küll (või vastupidiselt oskus puudus), kuid verifitseerimist takistas juba asjaolu, et nad ei olnud sellise võimaluse olemasolust teadlikudki. Jooniselt 4.7 näeme, et verifitseerimisest teadjate ja kõigi e-hääletajate grupiga tehtud regressioonianalüüside tulemused tegelikult üksteisest oluliselt ei erinenud, ent viimase puhul on tulemused tänu kitsamatele usaldusvahemikele natuke paremini tõlgendatavad.

4.2.1 Sotsio-demograafilised tegurid

Verifitseerimise tõenäosusele avaldas verifitseerimisest teadlike seas olulist mõju sugu, mille keskmine marginaalefekt oli 8% ± 5,4, ehk verifitseerimisest teadlikud mehed kasutasid verifitseerimist suurema tõenäosusega kui verifitseerimisest teadlikud naised (Joonis 4.7). Näeme, et samas suurusjärgus efekti tõotas omada ka emakeel, kuid laia usaldusvahemiku tõttu oli efekt statistiliselt ebaoluline. Kui vaatlusalust gruppi laiendati kõigi e-hääletajateni, saavutas ka emakeele efekt oodatud statistilise olulisuse. Näeme, et

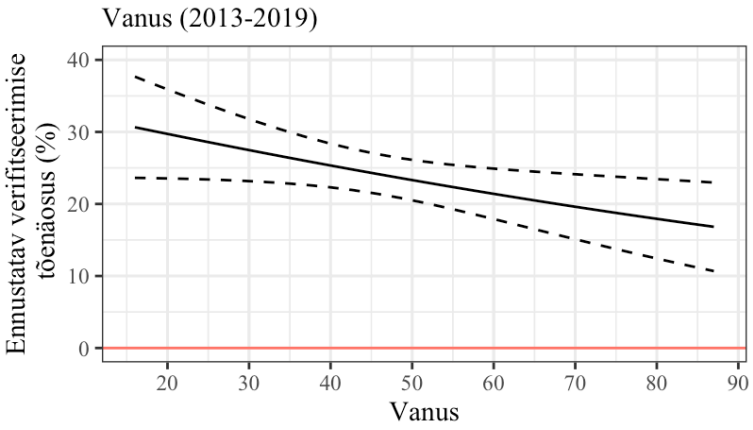
efekti suurus jäi grupi laiendamisel peaaegu samaks, mistõttu võib järeldada, et emakeel mõjutab samuti verifitseerimise tõenäosust – eestlane verifitseerib suurema tõenäosusega kui venelane.



Joonis 4.9 soo ja emakeele mõju valimiste lõikes (verifitseerimisest teadlikud e-valijad, 2013-2019)

Valimiste lõikes soo ja emakeele efekti suurused varieerusid, kuid olid verifitseerijate nappuse tõttu enamasti statistiliselt ebaolulised (Joonis 4.9). Üllatuslikult oli emakeele mõju statistiliselt oluline ja märkimisväärselt suur 2019. aasta Riigikogu ja Euroopa Parlamendi valimistel, mis viitab sellele, et tunnuse mõju võib olla ajaga hoopis süvenenud. See, kas tegu oli mingisuguse anomaaliaga või vastavate valimiste eripäraga, selle uurimuse kontekstis oluline ei ole. Difusiooni tuvastamise kontekstis on olulisim tähendada seda, et efektide suurused kummagi tunnuse ajas puhul kahanenud ei ole.

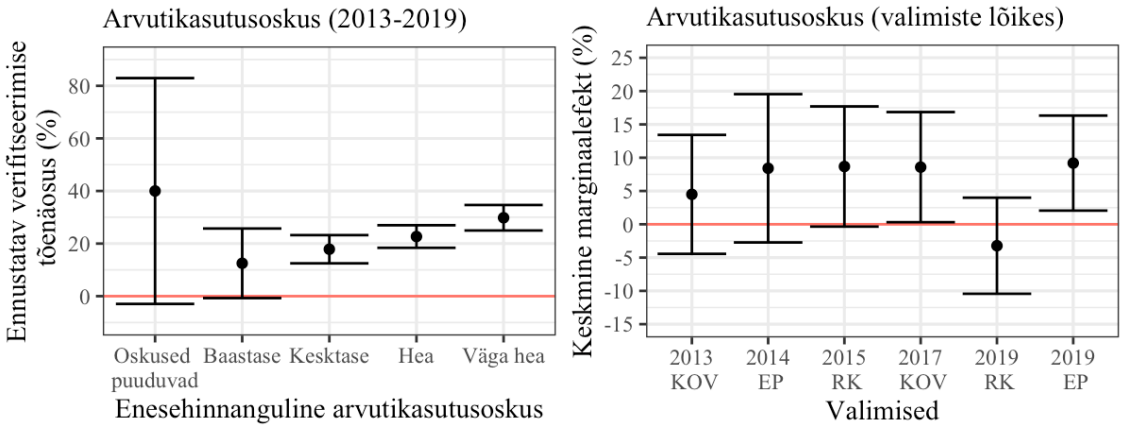
Kuigi joonisel 4.7 see esmapilgul ei avaldu, mõjutas verifitseerimise tõenäosust oluliselt ka vanus. Keskmine marginaalefekt näitab, mitme protsendi võrra tõuseb verifitseerimise tõenäosus sõltumatu tunnuse muutumisel ühe ühiku (faktori) võrra. Kuna vanus jaguneb hulga rohkemateks faktoriteks, kui sugu ja emakeel, siis ongi tunnuse keskmine marginaalefekt väga väike. Vanuse efekt tuleb selgemalt esile, kui vaadata otse, kui suur on tõenäosus teatud vanuses e-hääletajal verifitseerimist kasutada (Joonis 4.8).



Joonis 4.8: vanuse mõju verifitseerimise tõenäosusele (verifitseerimisest teadlikud e-hääletajad, 2013-2019)

Näeme, et mida noorem on verifitseerimisest teadlik e-hääletaja, seda suurema tõenäosusega ta verifitseerimist kasutab. Vanuse efekti uuriti ka valimiste lõikes (Lisa 1). Enamasti olid efekti suurused ja suunad sarnased kogu perioodi hõlmavale mudelile, aga 2014 EP ja 2019 RK valimistel oli efekt vastupidine – vanuse tõusuga suurenes tõenäosus verifitseerimist kasutada. Vanuse efekti suuruse kahanemist ajas märgata ei ole.

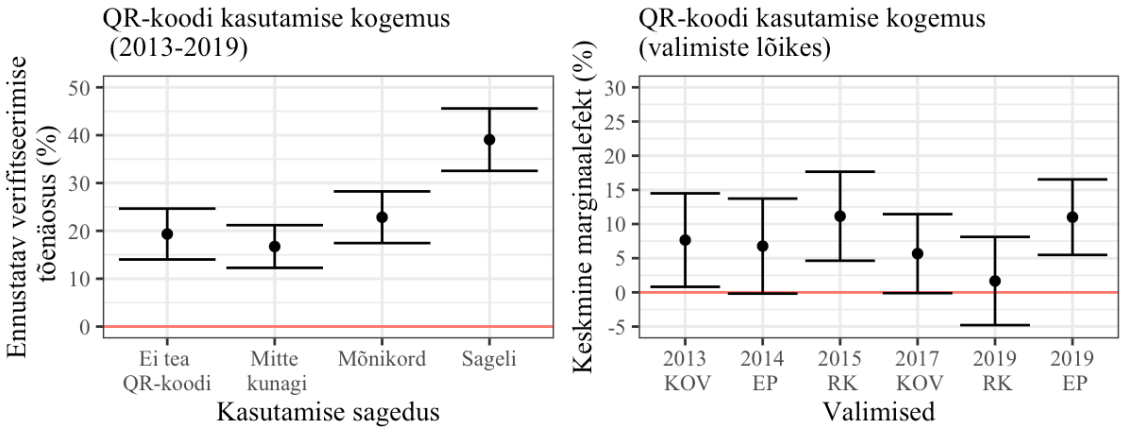
4.2.2 Digipädevust näitavad tegurid



Joonis 4.10: Arvutikasutusoskuse mõju verifitseerimise tõenäosusele (verifitseerimisest teadlikud e-hääletajad, 2013-2019)

Verifitseerimisest teadlike e-hääletajate seas mõjutasid verifitseerimise tõenäosust statistiliselt olulisel määral valija üldine arvutikasutusoskus (efekti suurus oli 5,4% ± 3,4) ning QR-koodi kasutamise kogemus (6,6% ± 2,5). Näeme, et mida kõrgem oli e-hääletaja enesehinnanguline arvutikasutusoskus, seda suurem oli tõenäosus, et ta kasutas verifitseerimist (Joonis 4.10). Statistiliselt olulisel määral tõusis verifitseerimise

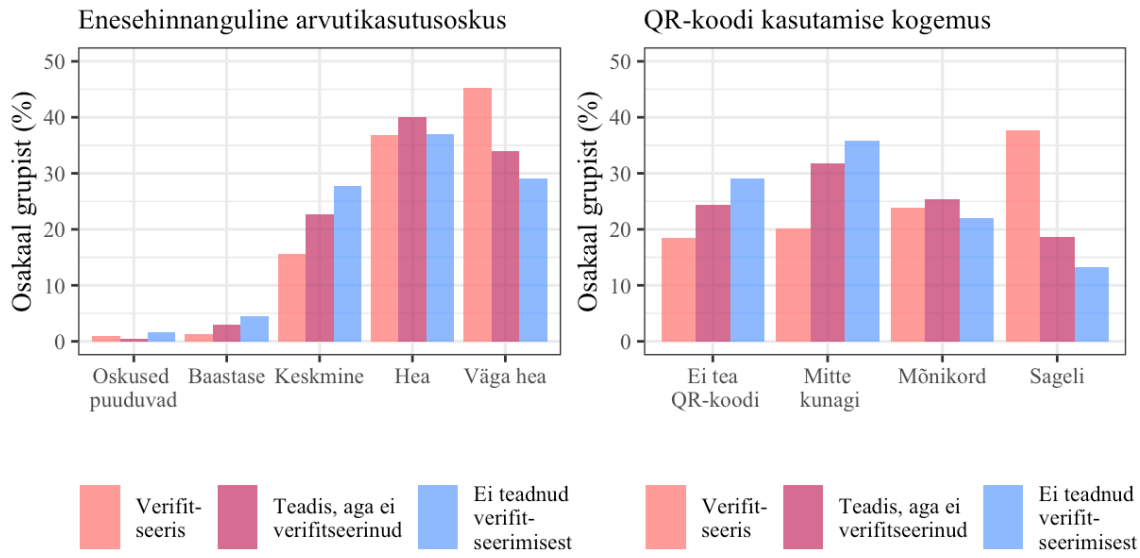
tõenäosus nendel valijatel, kes hindasid oma arvutikasutusoskust olevat keskmisel, heal või väga heal tasemel. Ajas tunnuse efekti muutust tähendada ei saa, sest valimiste lõikes oli efekt statistiliselt ebaoluline või väga nõrgalt oluline.



Joonis 4.11: QR-koodi kasutamise kogemuse mõju verifitseerimise tõenäosusele (verifitseerimisest teadlikud e-hääletajad, 2013-2019)

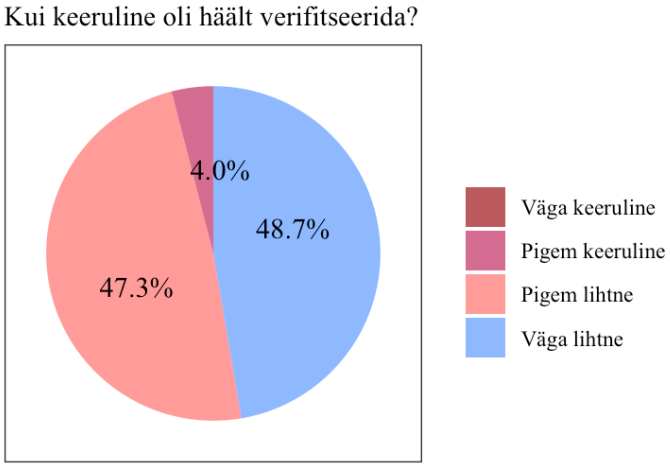
Joonis 4.11 kujutab QR-koodi kasutamise kogemuse mõju verifitseerimise tõenäosusele. Kogu perioodi vältel oli ennustatav verfitseerimise tõenäosus selgelt kõrgeim neil, kes olid QR-koodi kasutanud sageli (39,1% ± 6,5) ning madalaim neil, kes ei olnud QR-koodi kasutanud mitte kunagi (16,7% ± 4,4). QR-koodi kasutamise kogemuse mõju oli statistiliselt oluline kuuest valimisest kolmel, kuid selget trendi efekti olulisuse muutuses tähendada ei saa.

Jooniselt 4.12 on näha, et verifitseerinud e-hääletajate hulgas oli väga heal tasemel arvutikasutajaid protsentuaalselt rohkem, kui nende hulgas, kes ei verifitseerinud. Samuti oli verifitseerijate seas kõige rohkem selliseid valijaid, kes olid QR-koodi kasutanud sageli, ning kõige vähem neid, kes ei olnud QR-koodist kuulnudki. Verifitseerimisest mitte kasutanud e-hääletajate puhul oli tendents vastupidine – domineerisid need, kes ei olnud QR-koodi kasutanud mitte kunagi, ning kõige vähem oli valijaid, kes olid QR-koodi kasutanud sageli.



Joonis 4.12: Enesehinnanguline arvutikasutusoskus ja kogemus QR-koodi kasutamisega - jaotus kolme grupi seas (2013-2019)

Lisaks usaldust ja verifitseerimise tõenäosust mõjutavatele teguritele uuriti, kuidas hindasid verifitseerimise protsessi keerukust seda kasutanud e-hääletajad ise. Enamik verifitseerinud e-hääletajatest hindasid kasutamise protsessi väga lihtsaks või pigem lihtsaks (kokku 96% kasutajatest), vaid 4% leidsid, et rakendust oli pigem keeruline kasutada ning neid, kelle jaoks oli kasutamine väga keeruline, ei olnud üldse (Joonis 4.13).



Joonis 4.13: hinnanguline verifitseerimine keerukus (2013-2019)

5 Tulemused

5.1 Diskussioon

Analüüs näitas, et kogu e-valijaskonna usaldustase oli perioodil 2013-2019 tõusnud väga minimaalselt. Verifitseerimise olemasolust teadlike (sealhulgas verifitseerimist kasutanud) e-hääletajate keskmine usaldustase püsis kogu perioodi vältel kõrgem kui verifitseerimisest mitteteadlike e-hääletajate oma, kuid kui mitteteadlike e-hääletajate usaldustase ajapikku stabiilselt tõusis, siis teadlike e-hääletajate usaldustase oluliselt ei muutunud. See viitab sellele, et verifitseerimisest teadlike usaldustase võis juba eos kõrge olla ning kuna taseme muutus kajastub ainult mitteteadlike usalduses, siis verifitseerimine kogu e-valijaskonna usaldustaseme tõusu kindlasti ei seleta. Teisalt, nagu nentisid Solvak ja Vassil (2016: 135), võib verifitseerimisest teadjate usaldustaseme olematu tõus või koguni langus olla osaliselt tingitud ka sellest, et juba algselt kõrge usaldusega e-valijatel pole lihtsalt skaalal enam ruumi oma usaldust kõrgemalt hinnata. Muuhulgas selgus, et kogu e-valijaskonna usaldustaseme muutus nii verifitseerimiseelsel kui ka -järgsel perioodil oli minimaalne, kuid see on antud kontekstis pigem informatiivne ning viitab sellele, et keskmise e-valija usaldustase ajas eriti ei muutugi.

Valija usaldustaseme ja verifitseerimise vahelise seose seletamiseks uuriti verifitseerimise mõju kolmele tunnusele – usaldus e-valimiste vastu; usaldus, kas valija enda hääl läks arvesse; usaldus, kas teiste hääled läksid arvesse. Analüüs näitas, et kõigi kolme tunnuse põhjal oli verifitseerimisest teadlike usaldus märksa kõrgem kui verifitseerimisest mitteteadlike usaldus. Verifitseerimisest teadmise ja usalduse interaktsiooni lähemalt uurides selgus, et teadmise mõju on ajapikku kahanenud, sest verifitseerimisest teadlike usaldus ei ole ajas eriti muutunud, aga mitteteadlike usaldus on vahepeal tõusnud. Üllatuslikult selgus, et see kas teadlik valija ka tegelikult verifitseerib, usaldust endiselt olulisel määral ei mõjuta. Seega võib järeldada, et verifitseerimise vahel on seos, kuid see väljendub ainult verifitseerimisest teadjate ja mitteteadjate vahel – see, kas teadlik valija ka päriselt verifitseerimist kasutab, pole usalduse kontekstis oluline. Asjaolule, et verifitseerimisest teadmine võib usaldust mõjutada rohkem kui kasutamine, viitasid nii Solvaku ja Vassili (2016: 140-141) varasemad järeldused kui ka üldine teooria. Valija võib tajuda, et tal ei ole vaja oma häält verifitseerida, sest kui seda teeb edukalt keegi

teine, on see juba märk sellest, et süsteem on turvaline ja aus. Verifitseerijate hulk oli proportsionaalselt marginaalne ja verifitseerimise kasutamise väike või koguni olematu efekt valija usaldusele oli ka oodatav.

Selleks et ennustada, kas verifitseerimise kasutajaskond oli vahepeal muutunud, tugineti Everett Rogersi (2003) tehnoloogilise difusiooni teooriale, mis osutas sellele, et verifitseerimise puhul jääb vajaka mitmetest omadustest, mis soosivad difusiooni kulgu. Seetõttu ei kaota verifitseerijale iseloomulikud tunnused ajapikku oma olulisust, sest uusi adopteerijaid on vähe või ei ole üldse. Analüüsi põhjal ei saanud arvutikasutusoskust väljendavate ega ka sotsio-demograafiliste tegurite puhul efekti suuruse kahanemist ajas tähendada, sest valimiste lõikes vaadelduna olid efektid enamasti statistiliselt ebaolulised. Kogu perioodi hõlmavad mudelid näitasid seevastu, et kõik valitud tunnused ikkagi mõjutasid vähemal või rohkemal määral verifitseerimise tõenäosust. Sotsio-demograafiliste tunnuste mõjuanalüüs näitas, et tüüpiline verifitseerija kaldub olema nooremapoolne meessoost eestlane. Digipädevust näitavate tegurite mõju oli samuti arvestatav – e-hääletajate seas eristas verifitseerijat kõrgem enesehinnanguline arvutikasutusoskus ja eelnev kogemus QR-koodi kasutamisega. Tüüpiline verifitseerija on seega nende tunnuste poolest keskmisest e-valijast selgelt eristuv, kuid kuna verifitseerijaid on nii proportsionaalselt kui ka arvuliselt niivõrd vähe, siis valimiste kaupa see erinevus veel ei avaldu. Analüüsi põhjal võib kindlalt väita, et verifitseerimine on Eestis alles väga varajases innovatsioonijärgus ning seda kasutab eelmainitud spetsiifiliste tunnustega varajaste adopteerijate grupp.

Tulemused on kooskõlas teooriaga, mis viitas sellele, et tüüpiline verifitseerija sarnaneb algsele e-valijale. Kuna e-hääletamine on levinud tunduvalt laiema kasutajaskonna seas kui verifitseerimine, peaks spetsiifilisema taustaga verifitseerija keskmisest e-valijast eristuma. Teda peaks iseloomustama juba eos kõrge usaldus tehnoloogiliste innovatsioonide, sealhulgas e-valimiste vastu, mistõttu verifitseerimine tema usaldustaset enam oluliselt tõsta ei saagi. Analüüs viitas sellele, et verifitseerimist kasutab endiselt see sama spetsiifilise taustaga tehnoloogiahuviline valija, kellel sellest pealtnäha mingit kasu ei ole, sest tema usaldus e-valimiste vastu on niigi kõrge. Kohati jätab selline tendents mulje, et verifitseerimist kasutatakse pigem sellepärast, et tegu on mingi uudse ja põneva tehnoloogilise lahendusega, mida võiks moe pärast järgi proovida. Rakenduse sisuline funktsionaalsus jääb aga kasutaja motiivides tagaplaanile.

Verifitseerimist on sageli peetud ebapopulaarseks selle protseduurilise keerukuse tõttu (Kulyk & Volkamer 2018: 66-67). Analüüs näitas, et Eesti verifitseerimissüsteemi puhul see nii ei ole – vaid 4% verifitseerimist kasutanud vastajatest hindas rakenduse kasutamist pigem keeruliseks protsessiks ning väga keeruliseks ei hinnanud seda mitte keegi. Seetõttu tuleks kasutajate nappuse põhjuseid otsida mujalt. Süüdlaseks võib osutuda näiteks see, et teatud valija leiab, et tal ei ole vaja verifitseerida, kui teised seda teevad, mistõttu talle piisab juba teadmisest, et selline asi on olemas. Selline lähenemine seletaks natuke seda, miks verifitseerimisest teadjaid on võrdlemisi palju, tegelikke kasutajaid aga väga vähe. Asjaolu, et verifitseerimine ei ole laiema e-valijaskonna seas juba kuute valimiste jooksul levima hakanud, võib olla märk sellest, et praegusel kujul ei hakka verifitseerimine kunagi valija usaldust arvestataval määral tõstma. Selge on see, et tulevikus on vaja teha mingisuguseid arendajapoolseid samme rakenduse läbipaistvuse ja kasutajasõbralikkuse tõstmiseks. Vastasel juhul tuleb leppida sellega, et hääle verifitseerimise võimalusest saab praktilist kasu ainult süsteemi administraator.

5.2 Vastused uurimisküsimustele ja hinnangud hüpoteesidele

K1. Kuidas erineb verifitseerimist kasutanud e-hääletajate usaldus a) verifitseerimisest teadlike usaldusest b) verifitseerimisest mitteteadlike usaldusest?

H1. Nende usaldus, kes verifitseerimisest teadsid, on kõrgem kui nende usaldus, kes verifitseerimisest ei teadnud. Verifitseerimist päriselt kasutanud e-hääletajate usaldustase on omakorda pisut kõrgem, kui teadlike usaldus.

Hüpoteesis esitatud vahekorrad osutusid sisuliselt tõeseks, aga analüüs näitas, et kuigi verifitseerijate ja verifitseerimisest teadlike usaldustasemed erinesid, siis see, kas teadlik valija ka päriselt verifitseerimist kasutas, usaldust enam olulisel määral ei tõstnud. Verifitseerimisest teadmise mõju usaldusele on ajapikku kahanenud, mis tähendab, et kui varem oli verifitseerimisest teadjatel selgelt kõrgem usaldus kui mitteteadjatel, siis paistab, et ka teadmise mõju on tänaseks marginaliseerunud.

K2. Kuidas on e-valijaskonna usaldustase peale verifitseerimise võimaluse lisandumist muutunud?

H2. E-valijaskonna usaldustasemes muutus ei kajastu, sest verifitseerimist kasutab väga väike hulk e-valijaid, kelle usaldustase kipub niigi kõrge olema.

Hüpotees osutus tõeseks. Kogu e-valijaskonna keskmise usaldustaseme minimaalne tõus oli tingitud eelkõige nende valijate usalduse tõusust, kes verifitseerimisest ei teadnud. Verifitseerimist kasutab protsentuaalselt väga väike hulk inimesi, kelle usaldus kipub teooria järgi olema niigi kõrge. Seetõttu ei mõjuta verifitseerimine e-valijaskonna usaldustaset peaaegu üldse.

K3. Millised tunnused iseloomustavad „tüüpilist verifitseerijat“ ning kas nende mõju verifitseerimise tõenäosusele on viimase kuue valimise jooksul muutunud?

H3. Tüüpiline verifitseerija sarnaneb algsele tüüpilisele e-valijale: nooremapoolne keskmisest parema arvutikasutusoskusega eestlane, kellel on e-valimiste suhtes kõrge usaldus. Tunnuste olulisus ei ole ajapikku kahanenud, sest verifitseerimise difusioon kulgeb aeglaselt või ei kulge üldse.

Hüpotees osutus tõeseks. E-valijate seas paistsid verifitseerijad silma parema QR-koodi kasutamise kogemuse ja arvutikasutusoskusega. Samuti eristas verifitseerijaid keskmisest e-hääletajast kõrgem usaldus e-valimiste vastu. Sotsio-demograafiliselt kattub tüüpiline verifitseerija olulisel määral algse e-valija tüübiga – meessoost nooremapoolne eestlane. Tunnuste efektide suuruse muutust ajas tähendada ei saanud, sest valimiste lõikes olid efektid enamasti statistiliselt ebaolulised.

Kokkuvõte

Töö eesmärk oli empiirilistele andmetele tuginedes uurida, kas 2013. aastal implementeeritud individuaalse hääle verifitseerimine on e-valija usaldustaset e-valimissüsteemi vastu tõstnud. Analüüs näitas, et verifitseerimist kasutanud e-hääletaja usaldus e-valimiste vastu oli tõepoolest pisut kõrgem kui keskmisel e-hääletajal. Teooriaga kõrvutatuna viitasid tulemused aga sellele, et verifitseerimine ise selle kasutajate ega ka kogu e-valijaskonna usaldust oluliselt ei mõjutanud, sest verifitseerijate usaldustase kipub juba eos kõrge olema. Verifitseerimise ja usalduse vahelise interaktsiooni ammendavaks seletuseks oli seejuures tarvilik uurida ka rakenduse kasutajabaasi ja levikut Eesti ühiskonnas. Selle tulemusena leiti, et verifitseerimisrakendus on Eestis väga varajases innovatsioonijärgus. Selle tüüpiliseks kasutajaks osutus on nooremapoolne meessoost eestlane, keda iseloomustab muuhulgas väga hea arvutikasutusoskus ja eelnev kogemus QR-koodi kasutamisega.

Solvak ja Vassil uurisid verifitseerimise efekti ajal, mil see ei olnud veel piisavalt pika aja jooksul kasutust leidnud, ning avaldasid lootust, et ehk võetakse verifitseerimine ühiskonnas ajapikku ka laiema kasutajaskonna seas omaks (Solvak & Vassil 2016: 141). Käesoleva töö tulemused on olulised, sest need viitavad sellele, et kuigi verifitseerimist on kasutatud nüüdseks juba kuutel valimistel, ei ole see ikkagi jõudnud nende valijateni, kellel sellest tegelikult kasu võiks olla.

Verifitseerimise kasutamine e-hääletaja usaldust arvestataval määral ei mõjuta, kuid analüüsi käigus selgus, et valija usaldusele avaldab kohati mõju verifitseerimise võimalusest teadmine. Käesoleva töö mahulised ja sisulised limitatsioonid ei võimaldanud autoril teadmise efekti põhjalikumalt uurida, seega võiks valija usalduse ja verifitseerimisest teadmise vaheline seos olla suund edaspidisteks usaldust ja verifitseerimist käsitletavateks uurimusteks.

Kasutatud kirjandus

Al-Shammari, Ali Fawzi Najm, Adolfo Villafiorita & Komminist Weldemariam. 2012. „Towards an Open Standard Vote Verification Framework in Electronic Voting Systems.“ In *2012 Seventh International Conference on Availability, Reliability and Security*. Praha: IEEE, 437-444.

Avgerou, Chrisanthi. 2013. „Explaining Trust in IT-Mediated Elections: A Case Study of E-Voting in Brazil.“ *Journal of the Association for Information Systems* 14 (8): 420-451.

Bachmann, Reinhard & Akbar **Zaheer**. 2006. *Handbook of Trust Research.* Cheltenham, UK & Northampton, MA, USA: Edward Elgar.

E-hääle kontrollimine. https://www.valimised.ee/et/e-hääletamine/e-hääle-kontrollimine (külastatud 26. aprill, 2020).

Elektoonilise hääletamise statistika. https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-hääletamise-statistika (külastatud 26. aprill, 2020).

Gibson, J Paul, Robert Krimmer, Vanessa Teague & Julia Pomares. 2016. „A review of E-voting: the past, present and future.“ *Ann. Telecommun.* 71: 279-286.

Heiberg, Sven & Jan **Willemson**. 2014. „Verifiable Internet Voting in Estonia.“ In *2014 6th International Conference on Electronic Voting: Verifying the VOTE (EVOTE)*, Lochau: IEEE, 1-8.

Joaquim, Rui, Paulo Ferreira & Carlos Ribeiro. 2013. „EVIV: An end-to-end verifiable Internet voting system.“ *Computers & Security* 32 (veebruar): 170-191.

Kee, Herbert W. & Robert E. **Knox**. 1970. „Conceptual and methodological considerations in the study of trust and suspicion.“ *Journal of Conflict Resolution*, 14 (3): 357-366.

Kulyk, Oksana & Melanie **Volkamer**. 2018. „Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability.“ In *Third Joint International Conference on Electronic Voting.* Tallinn: TalTech Press, 66-81.

McKnight, D. Harrison, Michelle Carter, Jason Bennett Thatcher & Paul F. Clay. 2011. „Trust in a specific technology: An investigation of its components and measures.“ *ACM Transactions on Management Information Systems* 2(2): artikkel 12, 25 lk.

Popoveniuc, Stefan, John Kelsey, Andrew Regenscheid & Poorvi Vora. 2010. „Performance Requirements for End-to-End Verifiable Elections.“ In *Proceedings of the 2010 international conference on Electronic Voting Technology/Workshop of Trustworthy Elections (EVT/WOTE'10)*, 1-16.

Rogers, Everett M. 2003. *Diffusion of Innovations. Fifth Edition*. Free Press, New York.

Rura, Lauretha, Biju Issac & Manas Kumar Haldar. 2011. „Online Voting Verification with Cryptography and Steganography Approaches.“ In *Proceedings of 2011 International Conference on Computer Science and Network Technology*. Harbin: IEEE, 125-129.

Solvak, Mihkel & Kristjan **Vassil**. 2016. *E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005 - 2015)*. Johan Skytte Institute of Political Studies, Tartu.

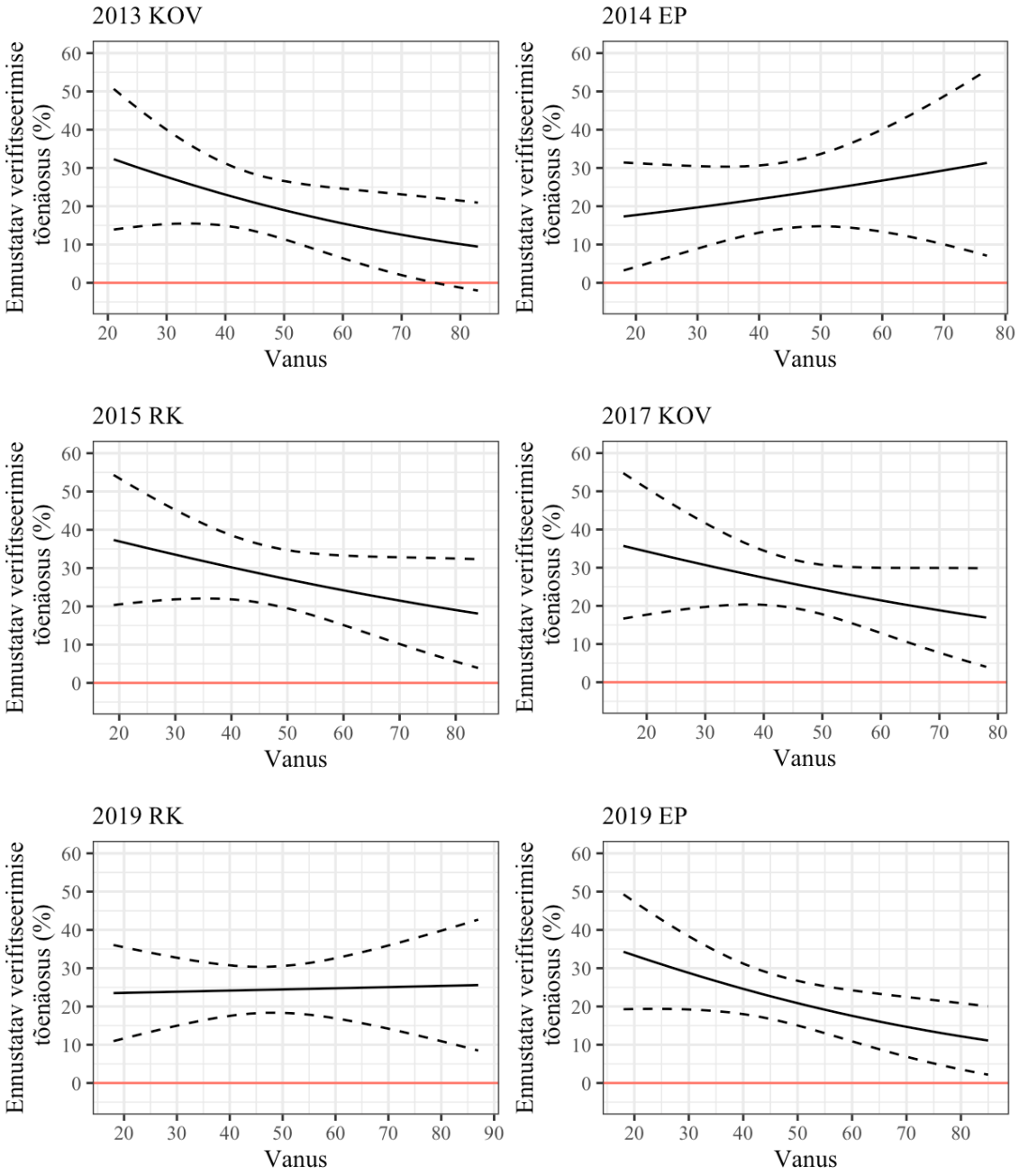
Vabariigi Valimiskomisjon. 2013. „Elektroonilise hääletamise süsteemi üldkirjeldus.“, 18. september, https://www.valimised.ee/sites/default/files/uploads/eh/elektroonilise-haaletamise-systeemi-yldkirjeldus-EH-03-03-1_2013.pdf (külastatud 26. aprill, 2020).

Vassil, Kristjan, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel & R. Michael Alvarez. 2016. „The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015.“ *Government Information Quarterly* 33 (3): 453-459.

Warkentin, Merrill, Shwadhin Sharma, David Gefen, Gregory M. Rose & Paul Pavlou. 2018. „Social identity and trust in internet-based voting adoption“ *Government Information Quarterly* 35 (2): 195-209.

Lisad

Lisa 1. Vanuse efekti muutus verifitseerimise tõenäosuse suhtes valimiste lõikes



THE EFFECT OF INDIVIDUAL VOTE VERIFICATION ON TRUST IN E-VOTING

Peeter Leets

Summary

Since 2005, Estonia has allowed their citizens to cast legally binding votes over the Internet. Due to the complicated and masked nature of online transactions, the demand arose for a reliable security mechanism to oversee the virtual voting process. This mechanism, known as end-to-end vote verification, has been in use since 2013 and its primary purpose is to detect malware attacks against the e-voting system. However, in theory, verification also has a user-oriented functionality – it should increase trust levels of the electorate by confirming e-voters that the system represents their true choice.

The interaction between verification and voter trust in Estonia has been briefly studied by Mihkel Solvak and Kristjan Vassil (2016). They concluded from data based on three consecutive elections that verification was yet to show an effect on trust because it was mainly used by young tech-savvy voters with high levels of trust to begin with. Since their study, three more elections in three years have taken place, which in the fast-paced domain of technology is a considerable amount of time for things to change. This suggested that another focused research could shed more light on what impact verification really has on the trust levels of e-voters.

This research used empirical data from six post-election surveys in conformity with several theories that explain trust in e-voting systems and technological advancements in general, to find out whether verification has started to 1) diffuse among the wider electorate and 2) increase voter trust levels. Statistical analysis based on six post-election surveys showed that even though verification has been used in six nation-wide elections by now, the results are largely identical to those presented by Solvak and Vassil. Verification is mostly used by people with a very distinct sociodemographic background, good computer skills and a disposition to trust the e-voting system. This suggests that verification still has little to no impact on increasing voter trust. Furthermore, it was revealed that verification does not show any obvious signs of diffusion, which could mean that verification may never be able to fulfil its trust-building purpose in its current form.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Peeter Leets (isikukood: _____) annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Individuaalse hääle verifitseerimise võimaluse mõju usaldusele e-valimiste vastu“, mille juhendaja on Mihkel Solvak,

1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace'is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
2. üldsusele kättesaadavaks tegemiseks ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
3. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;
4. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 15.05.2020

Peeter Leets, 15.05.2020